Informaatioteknologian tiedekunnan julkaisuja
No. **60**/2018

Petri Vähäkainu, Martti Lehto ja Pekka Neittaanmäki

Tekoäly ja kyberturvallisuus

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 60/2018

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7557-9 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2018

Tekoäly ja kyberturvallisuus

Raportti

Petri Vähäkainu
Martti Lehto
Pekka Neittaanmäki
21.12.2018

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2019

Tämä tutkimus on tehty Business Finlandin tukemassa WHC hankkeessa.

Business Finland-hanke: WHC

KUVAT

SISÄLLYSLUETTELO

LYHENTEET

AI	Artificial Intelligence eli tekoäly
ANN	Artificial Neural Network eli keinotekoinen neuroverkko
CT	Convolutional Neural Network eli konvoluutioneuroverkko
DMZ	Demilitarized Zone tarkoittaa fyysistä tai loogista aliverkkoa, joiden avulla yhdistetään organisaation oma tietojärjestelmä esimerkiksi Internetiin
DNS	Domain Name System on Internetin nimipalvelujärjestelmä, jonka tehtävänä on muuntaa verkkotunnuksia IP-osoitteiksi
DOS	Denial of Service tarkoittaa palvelunestohyökkäystä, jossa pyritään estämään esimerkiksi verkkosivuston käyttö kohdistamalla siihen paljon liikennettä
DDoS	Distributed Denial of Service on hajautettu useasta lähteestä tapahtuva hyökkäys, jossa käytetään usein kaapatuista tietokoneista koostuvaa Botnetiä
EW	Electronic Warfare tarkoittaa elektronista sodankäyntiä, jonka operaatioihin kuuluu mm. elektroniset hyökkäykset, suojaus ja sodankäynnin tuki
FNN	Feed Forward Neural Network tarkoittaa eteenpäin syöttävää neuroverkkoa
ITU	International Telecommunication Union on kansainvälinen YK:n alainen virasto, jonka tarkoituksena on koordinoida telealan operaatioita ja palveluita
IW	Information Warfare, informaatiosodankäynti
LAN	Local Area Network on rajoitetulla maantieteellisellä alueella toimiva yhden talon tai yrityksen muodostama tietoliikenneverkko
LAS	Laboratory Automation System eli automaattinen laboratoriojärjestelmä, joka kykenee sulkemaan kriittiset järjestelmät ja laitteet
MITM	Man-in-the-middle-hyökkäys tarkoittaa tietoturvahyökkäystä, jossa hyökkääjä asettuu kahden osapuolen välisen tietoliikenteen välittäjäksi
SIEM	Security Information and Event Management on järjestelmä organisaation tietojärjestelmien- ja verkkojen sekä poikkeamien tarkkailuun
SSL	Secure Socket Layer on ollut laajalti käytetty salausprotokolla, jolla suojattiin tietoverkkoliikennettä ennen v. 1999 julkaistua TSL-protokollaa
SOP	Same Origin Policy on selainten valvoma saman alkuperän turvarajoitus
TSL	Transport Layer Security on salausprotokolla, jonka avulla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli
VPN	Virtual Private Network eli virtuaalinen erillisverkko, jonka avulla voidaan yhdistää kaksi tai useampi yrityksen verkkoa tai käyttäjää toisiinsa

JOHDANTO

Tämän raportin tarkoituksena on tarkastella, miten tekoälyä voidaan hyödyntää kyberturvallisuuden alueella esimerkiksi ennustamaan ja estämään tulevia tietoverkkohin kohdistuvia hyökkäyksiä, tunnistamaan ja priorisoimaan potentiaalisia tietoturvauhkia sekä löytämään mahdollisia poikkeavuuksia. Tekoälystä esitellään raportissa sen määritelmä, hyötyjä ja haittoja, menetelmiä neuroverkoista syväoppimiseen saakka sekä sen hyödyntämisen eri alueita. Raportissa määritellään myös kyberturvallisuuden ja -avaruuden käsitteet, kyberturvallisuuden kehityskaari suurtietokoneiden aikakaudesta Internet-aikakauteen saakka sekä kyberturvallisuuden riskejä, uhkia ja haavoittuvuuksia. Raportin varsinaisena tarkastelun kohteena ovat tekoälyä hyödyntävät kyberturvallisuusratkaisut, joita esitellään raportin viimeisessä luvussa.

Tekoäly (engl. Artificial Intelligence eli AI) oli alkujaan muotisana, joka tarkoitti ihmisaivojen jäljittelemistä ja reaalimaailman ongelmien tutkimista holistisen ihmiskeskeisen lähestymistavan kautta. Tutkijat ja tiedemiehet ympäri maailman ovat innoissaan innovaation kehitysaskelista. Kehitysaskeleet ovat peräisin ihmiselle luontaisesta halusta kehittää uusia ja parempia teknologioita, jotka mahdollistavat ihmiskunnan ylittää sen fyysiset kyvyt. Lupaus tekoälyn käsitteestä on aina ollut horisontissa sekä reaalitodellisuuden tiedemaailmassa, että fiktiossa elokuvien ja kirjallisuuden kautta. (Kannan, 2017)

Tekoäly mahdollistaa suurten datamäärien varastoinnin sekä prosessoinnin älykkäällä tavalla ja se nimenomaan muuntaa relevanttia informaatiota funktionaalisiksi työkaluiksi. Tekoälyä on käytetty hyvin monella sovellusalueella, joista tunnetuimpia kenties ovat puolustuksen (kyberturvallisuus) ja avaruuden tutkimuksen alueet, joissa menestys ongelmien ratkaisemisessa tietyillä osa-alueilla on ollut erinomaista. Tekoälyn sovellusalue on sittemmin laajentunut terveydenhuoltoon, jossa sitä hyödynnetään muun muassa diagnosoinnissa, hoitosuosituksien tekemisessä, leikkaushoidossa ja niin edelleen. (Kannan, 2017) Uusiin tekoälyä hyödyntäviin aluevaltauksiin kuuluu myös tekoälyn ja sen menetelmien hyödyntäminen rakennusten terveydentilan (Structural Health Management eli SHM) tutkimisessa, jossa tekoälyn avulla voidaan tehdä tulevaisuutta koskevia ennusteita ja siten säästää korjauskustannuksissa.

Tekoäly ei kuitenkaan ole mitenkään uusi käsite, vaan se on kulkenut pitkän tien aina Alan Turingin koneesta nykypäivän kognitiivisiin tekoälyä hyödyntäviin innovaatioihin saakka. Toisen maailmansodan aikoihin Alan Turing alkoi kehittää teknologioita, kuten neuroverkkoja, jotka mahdollistavat tekoälyn sellaisena kuin me sen nykypäivänä tunnemme. Tekoäly voidaan käsittää eräänalaisena sateenkaariterminä, jonka tarkoituksena on saada tietokoneet ajattelemaan ihmisten kaltaisesti ja simuloimaan ihmisten tekemiä asioita sekä ratkaisemaan ongelmia nopeammin ja paremmin kuin ihmiset niitä kykenevät ratkaisemaan. Tekoälyä hyödyntäen voidaan suorittaa erilaisia tehtävätyyppejä, kuten luovia tehtäviä, suunnittelua, liikkumista, puhumista, objektien ja äänien tunnistamista, sosiaalisten ja liiketoiminnalisten transaktioiden suorittamista jne. Tehtätyyppien suorittamiseksi on mahdollista hyödyntää erilaisia menetelmiä, kuten evi-

denssipohjaiset menetelmät, luonnollisen kielen prosessointi, tekstin louhinta, prediktiivinen ja preskriptiivinen analytiikka, suosittelujärjestelmät sekä kone- ja syväoppiminen. Edellä mainittuja tekoälyä hyödyntäviä menetelmiä voidaan soveltaen käyttää myös kyberturvallisuuden ongelmien ratkaisemiseen.

Kyber tarkoitta ympärillämme olevaa digitaalista biteistä koostuvaa keinotekoista maailmaa, johon kuuluvat muun muassa Internet ja sosiaalinen media, erilaiset tietoverkot ja järjestelmät, älylaitteiden ohjelmistot jne. Kyber-sana tulee kreikankielisestä sanasta kybereo tarkoittaen ohjaamista, opastamista ja hallitsemista. Kyberturvallisuus yleisesti viittaa kykyyn kontrolloida pääsyä verkossa sijaitseviin järjestelmiin sekä informaatioon, joita järjestelmät sisältävät. Lordin (2017) mukaan kyberturvallisuus viittaa teknologioihin, prosesseihin ja käytänteisiin, jotka on suunniteltu suojelemaan verkkoja, laitteita, ohjelmia ja dataa hyökkäyksiltä, vahingoilta tai luvattomalta käytöltä. Kyberturvallisuutta voidaan myös kutsua informaatioteknologian turvallisuudeksi. Kaspersky lab:n (2018) mukaan kyberturvallisuus on tietokoneiden ja palvelinten, mobiililaitteiden, elektronisten järjestelmien, verkkojen ja datan turvaamisen käytäntö haitallisia hyökkäyksiä vastaan. Termi on laaja-alainen ja soveltuu kaikkeen tietokoneiden turvallisuudesta saakka katastrofeista toipumiseen ja loppukäyttäjien koulutukseen asti.

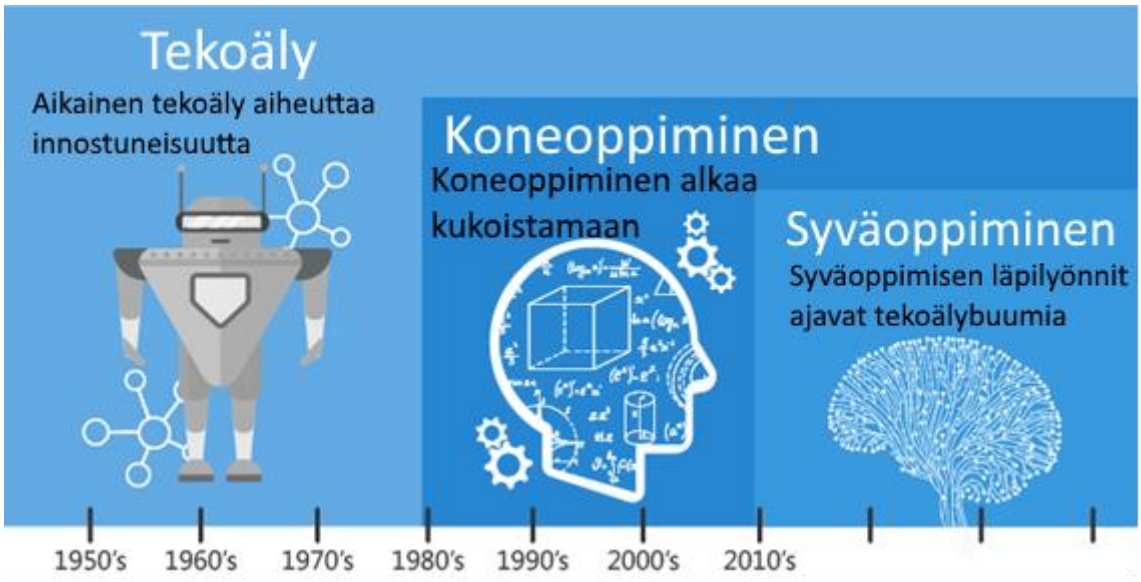
Organisaatiot ovat aloittamassa tekoälyn hyödyntämistä kyberturvallisuuden saralla tarjoten aiempaa parempaa tietoturvaa yhä taitavampia hyökkääjiä vastaan. Tekoäly auttaa automatisoimaan monimutkaisia prosesseja hyökkäysten tunnistamiseksi ja reagoimalla tietomurtoihin. Tämänkaltaiset sovellukset ovat kehittymässä entistä paremmiksi tekoälyn hyödyntämisen myötä. Koneoppiminen on yksi tekoälyn osa-alueista, joka viittaa teknologioihin, joiden avulla tietokoneet voidaan saada oppimaan ja mukautumaan kokemuksien kautta. Kyseinen teknologinen osa-alue simuloi ihmiskognitiota, kuten kokemuksista ja malleista oppimista päättelyn sijasta (syy ja seuraus). Nykyään syväoppimisen kehitysaskeleet koneoppimisen osa-alueella tarjoavat koneille mahdollisuuden oppia rakentamaan hahmontunnistuksen malleja ilman ihmisen sekaantumista. Uuden mallin tunnistusta voidaan verrata jo tunnettuihin malleihin, jotta potentiaalinen haitallisuustaso voidaan hahmottaa. Tunnistusprosessin nopeus ja tarkkuus eivät ole mahdollisia ihmisasiantuntijoille mielekkäässä ajassa.

Tässä raportissa on käsitelty eri valmistajien tekoälyä hyödyntäviä sovellusratkaisuja, jotka hyödyntävä tekoälyä tietoturvauhkien sekä anomalioiden ennustamisessa, tunnistamisessa ja estämisessä. Sovellusratkaisujen tarkasteluiden on tarkoitus antaa yleiskuva siitä, minkälaisia tekoälyä hyödyntäviä kyberturvallisuusratkaisuja on olemassa ja mitä ne voivat tarjota kyseistä aluetta käsittelevien ongelmien ratkaisemiseksi. Integroitu IBM Security-tietoturvaratkaisu on raportissa tarkastelluista ratkaisuista selkeästi laajin ja sen tarkoitus on auttaa organisaatioita tunnistamaan, kohdistamaan ja estämään tietoturvauhkia. Ratkaisun on tarkoitus olla kokonaisvaltainen ja sitä hyödyntäen organisaation tietoturva voidaan turvata tietoverkon turvaamisesta mobiililaitteisiin, sovelluksiin ja loppukäyttäjiin saakka. IBM Security-tietoturvaratkaisu hyödyntää IBM:n kehittämää Watson-tekoälyä, jota on aiemmin onnistuneesti hyödynnetty esimerkiksi lääketieteen diagnosoinneissa, kuten ihosyöpädiagnosoinneissa.

1 TEKOÄLY – KONEOPPIMISESTA SYVÄOPPIMISEEN

Neuroverkoista tulee mieleen helposti ajatus, että ne ovat uusimpien tietoteknisten innovaatioiden joukossa, mutta niiden kehitys alkoi jo samaan aikaan kuin ensimmäisten tietokoneiden kehitys 1950-luvulla. Tarve neuroverkkojen kehitykselle oli saada kielenkääntäminen automatisoitua, tosin merkittävää kehitystä kyseisellä alueella ei saatu aikaan, jolloin kehitys hidastui. Neuroverkkojen kehitys alkoi kukoistaa uudelleen 1980-luvulla, jolloin oli mahdollista saada uutta tietoa ihmisaivojen rakenteesta ja toiminnasta. Tämän lisäksi tietokoneiden suorituskyvyn nopea paraneminen on vaikuttanut neuroverkkojen kehitykseen positiivisella tavalla. (Bask ym., 1998)

Kuvasta 1 havainnollistuu tekoälyn kehityskulku, joka alkoi jo 50-luvulla. Tekoälyn termi on kyseisen aihealueen termeistä laajin, joka mahdollistaa tietokoneille matkia ihmisten älykkyyttä käyttämällä logiikkaa, jos-sitten (If-Then) -sääntöjä, päätöspuita, kone- ja syväoppimista. Koneoppiminen on tekoälyn osa-alue, joka käyttää tilastollisia teknologioita, jotka mahdollistavat koneiden oppivan kokemuksista. Kategoria sisältää myös syväoppimisen. Syväoppiminen on koneoppimisen osa-alue muodostuen algoritmeista, jotka mahdollistavat ohjelmiston itseoppimisen tehtävien suorittamiseksi, kuten puhe, kuvantunnistus jne. käyttämällä hyväksi neuroverkkoja suuren datamäärän käsittelemiseksi. (Parloff, 2016) (Copeland, 2016)



Kuva 1 Kehityskulku tekoälystä syväoppimiseen (Copeland, 2016)

1.1 Tekoälyn määritelmä

Tekoäly voidaan nähdä keinotekoisena älykkyytenä, jonka avulla voidaan ratkaista monimutkaisia ongelmia kyseisen järjestelmän ollessa tietokone tai kone. Tekoäly on tietotekniikan ja fysiologisen älykkyyden yhdistelmä, joiden avulla voidaan laskennallisesti päästä tavoitteisiin. Älykkyys on kyky ajatella luomalla muistia ja ymmärrystä, tunnistamalla malleja, tekemällä muutokseen sopeutuvia valintoja ja oppimalla kokemuksista. Tekoäly voi saada koneet käyttäytymään, kuten ihmiset, mutta paljon vähemmällä ajalla, mitä ihmiset käyttäisivät jonkin tietyn asian ratkaisemiseen. (Borana, 2016)

Tekoälyn juuret ovat pitkälti useilla eri tiedonaloilla, kuten:

- Biologia/neurotiede
- Filosofia
- Laskenta
- Logiikka
- Psykologia/kognitiotiede

Tekoäly alkoi kehittyä Turingin koneesta, jolla mitattiin koneen kykyä älykkääseen käytökseen. Turingin koneen esitteli Alan Turing julkaisussaan: ”Computing Machinery and Intelligence”. Testin peruskysymyksenä on: ”Voivatko koneet ajatella?”. Testissä asetelmana on kuulusteleva ihminen ja toisella puolella tietokone ja toinen ihminen, joita kuulustelija ei voi nähdä. Keskustelu käydään luonnollisella kielellä ja mikäli kuulustelija ei voi luotettavasti todentaa, onko kuulusteltava ihminen vai kone, kone on läpäissyt testin. Testi tehdään tekstimuodossa, jotta puheesta ei voi päätellä, kummasta on kyse. (Borana, 2016)

Tekoäly voidaan jakaa esimerkiksi seuraavalla tavalla sovellusalueisiin:

1. Kognitiivisen tieteen sovellukset
2. Robotiikan sovellukset
3. Luonnollisen kielen sovellukset

1.2 Tekoälyn hyötyjä ja haittoja

Osa “teknologiaguruista” on nostanut esiin tekoälyn kehittämisen haasteet. **Stephen Hawking** on todennut, että kokonaisvaltaisen tekoälyn kehittäminen voisi tietää ihmisrodun loppua. Päästyään vauhtiin, se kehittäisi itseään yhä kiihtyvällä vauhdilla. Ihmiset, joita hidas biologinen kehitys rajoittaa, eivät menestyisi kilpailussa ja ne syrjäytettäisiin. **Elon Musk** vertasi kehittyvää tekoälyä "demonin kutsumiseen" ja kutsui sitä ihmisrodun suurimmaksi eksistentiaaliseksi uhkaksi. Hän on myös twiitannut, että tekoäly voisi olla vaarallisempi kuin ydinaseet. **Nick Boström** väittää, että sen jälkeen, kun koneet ylittävät ihmisälyn, ne voisivat mobilisoitua ja päättää hävittää ihmiset erittäin nopeasti käyttäen erilaisia strategioita kuten näkymättömät taudinaiheuttajat, värväten ihmisiä omalle puolelleen tai yksinkertaisestikäyttäen raakaa voimaa. **James Barrat** väittää, että älykkäitä olentoja käytetään maapallon resurssien keräämiseksi, mikä väistämättä johtaisi supertekoälyn ja ihmisen väliseen resurssikilpailuun. (Lehto, 2017)

Tekoälyä käytettäessä siihen liittyy seuraavia riskejä ovat Lehdon (2017) mukaan:

- Ohjelmistotason riskit
- Laitetason riskit
- Algoritmiriskit
- Hallintariskit
- Eettiset riskit ja vastuukysymykset
- Yksityisyyden riskit

Tekoälyn algoritmit muodostavat riskiympäristön. Älykkäät autonomiset robotit toimivat annettujen ja opittujen algoritmien perusteella, kuten esimerkiksi sumea logiikka, sääntöjärjestelmät, geneettiset algoritmit, parveilualgoritmit. Algoritmien tavoitteena on mallintaa ihmisen ajattelua ohjelmallisin keinoin. Algoritmisuunnittelun haasteena on luoda eri tilanteet ja olosuhteet hallitseva algoritmi ja samalla antaa autonomiselle robotille kyky ihmismäiseen loogiseen ja analyyttiseen päätöksentekoon. Esimerkiksi robottiautoa on kielletty ajamasta päin punaisia. Käskyn myötä robottiauto saattaa ratkaista ongelman hakkeroimalla liikennevalojärjestelmään ja kääntämällä kaikki valot vihreiksi. Näin se omasta mielestään optimoi tehtävänsä. (Lehto, 2017)

OpenAI:n tutkija Ian Goodfellow totesi joulukuussa 2016 NIPS-konferenssissa (Neural Information Processing Systems), että tekoälypohjaisia järjestelmiä vastaan hyökkääminen on melko helppoa ja niiden puolustaminen on todella vaikeaa. Viime vuosina tutkijat ovat demonstroineet monia keinoja harhauttaa tekoälypohjaisia järjestelmiä hyödyntämällä niiden taipumusta erilaisten säännönmukaisuuksien havaitsemiseen datassa. Haavoittuvuus perustuu niiden algoritmiseen toimintatapaan eikä ihmismäiseen älykkyyteen. Itseohjautuvaa autoa hallitsevaa konenäkösovellusta voi esimerkiksi harhauttaa mainostaululla. Samoin puheohjatun sovelluksen voi saada tekemään ei-toivottuja asioita syöttämällä sille ääntä ihmisen kuuloalueen ulkopuolella olevalla taajuudella. (Lehto, 2017)

Tekoälyn hyötyjä (Borana, 2016):

- Tiedon jakaminen on helpompaa, sillä kun tekoäly on opetettu tietyn asian suhteen, se voidaan helposti kopioida, eikä ole tarpeen järjestää koulutuksia, kuten ihmisille.
- Toisin kuin ihmiset, koneet eivät tarvitse unta ja voivat työskennellä silloinkin, kuin ihmiset ovat jo väsyneet.
- Yksi tekoälyn parhaita hyötyjä on, että päätökset tehdään perustuen faktoihin, eikä tunteisiin, sillä yksi tunnetusti tunteet vaikuttavat ihmisten tekemiin päätöksiin negatiivisella tavalla.

Tekoälyn haittoja (Borana, 2016):

- Kykenemättömyys selittää tietyn päätöksen takana olevaa logiikkaa ja päättelyä.
- Luovuuden puute vastauksissa.
- Nykyinen kehitys on vielä sillä tasolla, että tekoäly ei kykene päättelemään, milloin tiettyyn ongelmaan ei ole ratkaisua.
- Terveen järjen puute päättelyssä voi johtaa suuriin ongelmiin.
- Toimintakyvyn häiriöt voivat johtaa tilanteeseen, jolloin tekoäly tuottaa vääriä ratkaisuja, sillä tekoäly ei kykene selittämään ratkaisuihin johtavaa päättelyä ko. tapauksessa.
- Väärissä käsissä tekoäly voi aiheuttaa massiivisen mittakaavan ongelmia.

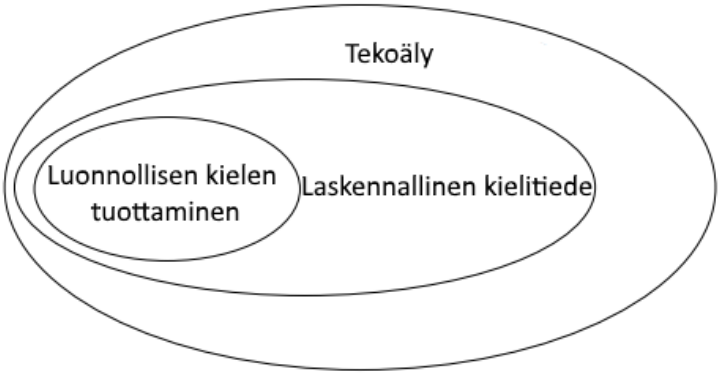
1.3 Tekoälyn menetelmiä

Tekoäly on kulkenut pitkän tien aina Alan Turingin koneesta nykypäivän kognitiivisiin tekoälyä hyödyntäviin innovaatioihin saakka. Alan Turing aikoinaan alkoi kehittää teknologioita, kuten neuroverkot, jotka tekevät tekoälyn, jona sen nykyään tunnemme, mahdolliseksi. Tekoäly on laaja sateenvarjotermi, jonka tarkoituksena on saada tietokoneet ajattelemaan, kuten ihmiset ajattelevat ja simuloimaan asioita, joita ihmiset tekevät ja lopulta ratkaisemaan ongelmia paremmin ja nopeammin kuin ihmiset kykenevät ratkaisemaan. Tehtävätyypit voivat olla muun muassa luovia tehtäviä, suunnittelua, liikkumista, puhumista, objektien ja äänien tunnistamista, sosiaalisten ja liiketoiminnallisten transaktioiden suorittamista. (Buczkowski, 2017) Edellä mainittujen tehtävätyyppien suorittamiseksi tekoälyä voidaan hyödyntää erilaisilla menetelmillä, joita ovat muun muassa evidenssipohjaiset menetelmät, luonnollisen kielen prosessointi, tekstin louhinta, prediktiivinen ja preskriptiivinen analytiikka, suosittelujärjestelmät, kone- ja syväoppiminen jne. (I-Scoop)

Evidensseihin perustuva ajattelutapa viittaa konseptiin tai strategiaan, joka on muodostettu objektiivisten todisteiden perusteella. Evidensseihin perustuva ajattelu riippuu todellisista kokeista tai testeistä, jotka todistavat, että strategialla tai konseptilla on todennäköisyys onnistua. Oletettavasti saatu informaatio johtaa päätöksentekijän valitsemaan parhaiten toimivan toimintatavan. Päätöksentekijät uskovat, että toimintatavan tulisi ratkaista jokin tietty ongelma ja johtaa haluttuun lopputulokseen. Evidenssipohjainen lähestymistapa sisältääkin avainkysymyksen: ”onko jokin tietty toimintatapa todistettu olevan tehokas muille samankaltaisissa tilanteissa?” Evidensseihin pohjautuvaa päätöksentekoa on onnistuneesti hyödynnetty muun muassa lääketieteessä, jossa todennäköisyys oikean hoitokäytänteen valitsemiseen evidensseihin perustuen on poistanut epävarmuustekijöitä, jolloin lääkärit ovat kyenneet määrittämään oikeanlaisen ja yhtenäisen hoitomuodon. (Lumen)

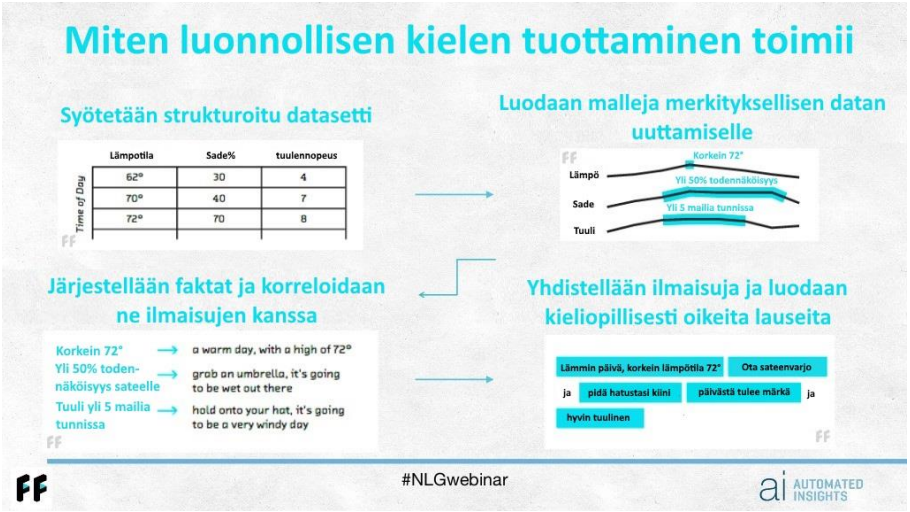
Tekoälyn osa-alueisiin kuuluu myös luonnollisen kielen prosessointi (Natural Language Generation eli NLG), jolla tarkoitetaan tekstitiedon tuottamista datasta. NLG on prosessi, jossa dataa tulkitaan tarkoituksenmukaisesti ja jossa se esitetään helposti ymmärrettävässä luonnollisen kielen muodossa tiettyjen määriteltyjen kommunikaatiotavoitteiden saavuttamiseksi. Tämänkaltaisia työkaluja käytetään, kun prosessoidaan laajoja

rakenteisessa tai rakenteettomassa muodossa olevia data-aineistoja. NLG-prosessin lopputuloksena saadaan luonnollisella kielellä esitetty teksti, joka on generoitu perustuen kerättyyn dataan ja käyttäjän tuottamaan syötteeseen. Luonnollisen kielen prosessointi toimii tietyllä tapaa vastakkaisena mallina luonnollisen kielen ymmärtämiselle (Natural Language Understanding eli NLU). NLG-prosessissa järjestelmä tekee päättelyitä, kuinka saattaa konsepti sanalliseen muotoon NLU-prosessin toimiessa päinvastoin. Kuvassa 2 havainnollistetaan luonnollisen kielen prosessointia osana laskennallista lingvistiikkaa, jotka molemmat muodostavat tekoälyyn kuuluvan osajoukon. (GeeksforGeeks)



Kuva 2 NLG tekoälyn ja laskennallisen lingvistiikan osajoukkona(Dale, 1995)

Kuvassa 3 on esimerkki luonnollisen kielen prosessoinnista. Syötteenä olevassa aineistossa on lämpötila (Fahrenheit), sademäärä (prosentteina) ja tuulen nopeus. Aineiston perusteella rakennetaan tietomalli, jonka avulla merkityksellinen informaatio saada avattua ymmärrettävään muotoon. Tämän jälkeen relevantti informaatio järjestetään, saatetaan se korreloimaan luonnollisen kielen lauseiden kanssa. Lopuksi lauseet yhdistetään kieliopillisesti oikeiksi lauseiksi, jolloin lopputuloksena on ymmärrettävä ja käyttökelpoinen teksti.



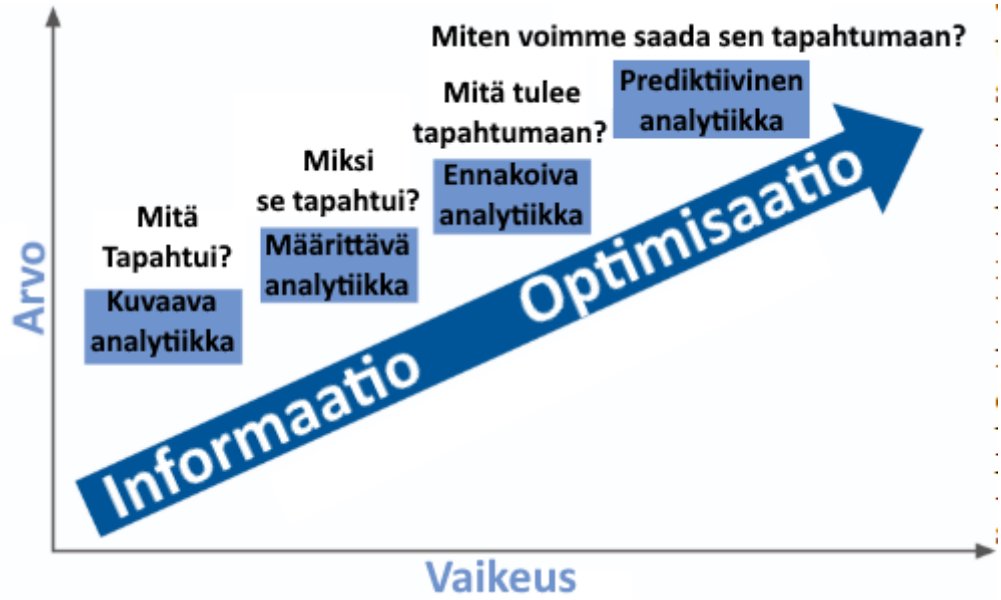
Kuva 3 Esimerkki luonnollisen kielen prosessoinnin toiminnasta (Allen & Mason, 2016)

Luonnollisen kielen prosessointi (Natural Language Processing eli NLP) on tutkimusala, jonka tutkimuksen kohteena on tietokoneiden kyky hyödyntää luonnollista kieltä, kuten puhetta tai tekstiä ja oppia tulkitsemaan niitä. Luonnollisen kielen tulkinta on tärkeää, mikäli tekoälyjärjestelmän halutaan vuorovaikuttavan ihmisten kanssa. NLP on käsitteenä ollut olemassa jo vuosikymmeniä ja se on kehittynyt useista eri teknologioista, jotka tyypillisesti ovat saaneet vaikutteita lingvistiikasta, jossa teksti on syntaktisesti jäsennelty hyödyntämällä muodollisia kielioppisääntöjä ja sanakirjaa. Lopputuloksena syntyvä informaatio on sen jälkeen semanttisesti tulkittu ja sitä on hyödynnetty halutessa tietää, mitä on sanottu eli mikä on informaation välittämä sanoma. NLP voi olla syvää, jolloin jäsennellään kaikki osat jokaisesta lauseesta ja koetetaan semanttisesti huomioida jokainen osa. NLP voi myös pinnallisempaa, jolloin jäsennellään vain tiettyjä sanontoja lauseessa tai tuotetaan ainoastaan rajoittunut semanttinen analyysi. NLP voi myös hyödyntää tilastollisia menetelmiä sananmuotojen tai sanontojen etsimisessä lauseesta. NLP:lle on tyypillistä, että sen yhteydessä keskitytään yhteen dokumenttiin tai tekstinosaan, joka voi laskennallisesti olla aikaa vievää. NLP-tekniikoita ovat muun muassa suffiksien (jälkiliite), perusmuotoistaminen (korvaa taivutetun sanan perusmuotoisella sanalla), monisanaelementtien ryhmittely, synonyymin normalisointi, sanojen merkityksen louhinta, roolin määrittäminen ja niin edelleen. (Kao & Poteet, 2005, 1)

Tekstin louhinta (text mining) on käsitteenä NLP:tä uudempi ja siinä käytettäviä tekniikoita on alkujaan kehitetty tiedonhankinnan alueella, tilastotieteessä ja koneoppimisessa. Sen tavoitteena ei ole saada ymmärrystä kaikesta tai edes suurimmasta osasta tekstin kirjoittajan välittämästä sanomasta, vaan ennemmin poimia malleja suuresta määrästä dokumentteja. Yksinkertaisin tekstin louhinnan muoto on informaation hakeminen, jota kutsutaan tekstin tai dokumenttien hakemiseksi, jota hakukoneet tyypillisesti käyttävät. Kuitenkin tekstin louhintaan kuuluu alueita, kuten automaattinen tekstin luokittelu joidenkin kiinteiden luokkien mukaisesti, kuten tekstin klusterointi, automaattiset yhteenvedot, aihealueiden louhinta teksteistä tai tekstiryhmistä ja trendien analysointi tekstivirroista. Tyypillinen tekstin louhinnan sovellus on luonnollisella kielellä kirjoitettujen dokumenttien läpikäyminen ja dokumenttiaineiston mallintaminen ennustavan luokittelun tarpeita ajatellen. (Kao & Poteet, 2005, 1)

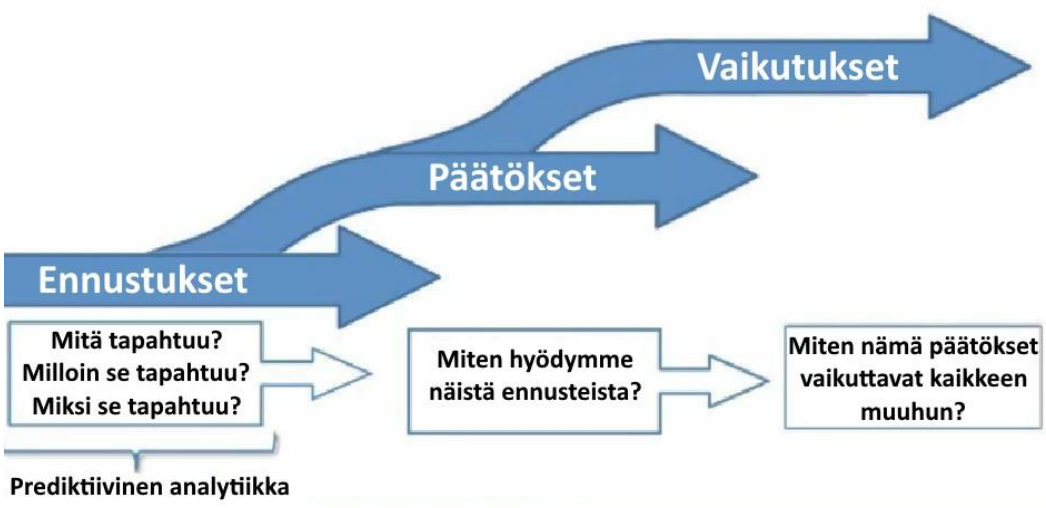
Prediktiivinen analytiikka (Kuva 4) on melko uusi menetelmä, joka antaa yrityksille mahdollisuuden saada tietoa reaaliajassa ja muodostaa prediktiivisiä ja preskriptiivisiä malleja, joiden avulla koko käytössä oleva data on hyödynnettävissä. Esimerkiksi Amazon suosittelee tuotetta ja Google kykenee ennustamaan, milloin henkilön tulisi tehdä lounaspöytävaraus, jotta se tulisi tehtyä ajoissa. Prediktiivistä analytiikkaa käytetään määrittelemään todennäköinen tulevaisuudessa ilmenevä tietystä tapahtumasta johtuva seuraus tai todennäköisyys tulevaisuudessa ilmenevän seurauksen tapahtumiselle. (Walker, 2016) Smeas Education Solutionsin (2013) mukaan prediktiivisen analytiikan voidaan katsoa olevan tiedonlouhinnan haara, joka ennustaa tulevaisuuden todennäköisyyksiä ja trendejä. Prediktiivistä analytiikkaa käytetään automaattisesti analysoimaan suuria määriä erilaisia muuttujia sisältävää dataa, kuten klusterointi, päätöspuut, ostoskorianalyysi, regressiomallinnus, neuroverkot, geneettiset algoritmit, tekstin louhinta, hypoteesin testaaminen, päätöksenteon analytiikka ja niin edelleen. Prediktiivinen analytiikka kykenee yhdistämään myös liiketoimintatietouden ja tilastollisen analytiikan

tekniikat uusien ideoiden saavuttamiseksi. Tämänkaltaiset ideat auttavat organisaatioita ymmärtämään, kuinka ihmiset käyttäytyvät esimerkiksi asiakkaina, ostajina, myyjinä ja jakelijoina.



Kuva 4 Prediktiivinen analytiikka menneisyydestä tulevaisuuteen (Allen & Mason, 2016)

Preskriptiivinen analytiikka (Kuva 5) on kehittyneen analytiikan muoto, joka tutkii dataa tai sisältöä vastatakseen kysymykseen: "Mitä tulisi tehdä?" tai "Mitä voimme tehdä, jotta saisimme tilanteen X tapahtumaan?" Preskriptiivinen analytiikka hyödyntää tekniikoita, kuten graafianalyysi, simulointi, monimutkaisten tapahtumien käsittely, neuroverkot, heurestiikka, koneoppiminen ja niin edelleen. (Gartner, 2018) IBM:n (2018) mukaan preskriptiivinen analytiikka on kehittynyt analytiikkateknologia, joka voi tarjota suosituksia päätöksen tekijöille ja auttaa heitä saavuttamaan liiketoiminnallisia tavoitteitaan ratkaisemalla monimutkaisia optimointiongelmia. Preskriptiivinen analytiikka auttaa organisaatioita tekemään parempia päätöksiä optimoimalla kaupallisia tavoitteita, kustannuksia ja asiakaspalvelua. Preskriptiivinen analytiikka arvioi saatavilla olevien resurssien ennusteita, sääntöjä ja rajoitteita, jotta se kykenee suosittelemaan parhaan mahdollisen toimintatavan. Walker (2013) kuvailee, että preskriptiivistä analytiikkaa voidaan hyödyntää terveydenhuollon alan strategisessa suunnittelussa analysoimalla operationaalista ja palveluiden käytön dataa. Ne ovat yhteydessä ulkoisiin tekijöihin, kuten taloudelliseen dataan, demograafisiin trendeihin ja väestön terveystrendeihin. Niiden avulla on mahdollista yhä tarkemmin suunnitella tulevaisuuden sairaalainvestointeja, kuten uudet rakennukset ja instrumenttien käyttö.



Kuva 5 Prediktiivinen analytiikka, päätöksenteko ja vaikutukset (Walker, 2013)

Suosittelujärjestelmät (recommendation engine) ovat informaation suodatinjärjestelmiä, jotka käsittelevät informaation ylikuormituksen muodostamia ongelmia suodattamalla elintärkeitä informaation palasia suuresta määrästä dynaamisesti generoitua informaatiota henkilön mieltymyksiin, kiinnostuksiin tai tarkkailtuun käytökseen liittyen. Suosittelujärjestelmällä on kyky henkilön profiilin perusteella ennustaa, pitääkö tietty henkilö jostain tietystä tuotteesta tai tavarasta. Ennustaminen varmistaa, että asiakas saa nähtäväksi hänen makunsa suhteen relevanttia dataa, joka voi olla esimerkiksi maku, tyyli tai muita ominaisuuksia, jotta oikeanlaisen datan etsimineen ei kuluisi aikaa. Suosittelujärjestelmät kykenevät jatkuvasti oppimaan uutta ja sopeutumaan uusiin asiakkaiden käyttäytymismalleihin. (Naik, 2017)

Suosittelujärjestelmän suosio alkoi kasvaa vähittäiskaupassa, pääasiassa online-kaupankäynnissä henkilökohtaisten tuotesuositteluiden muodossa. Yksi yleisimmistä käyttötarkoituksista on Amazonin suosittelujärjestelmä, joka informoi asiakasta tyyliin: "asikas, joka osti tämän tuotteen, osti myös...". Suosittelijajärjestelmä on älykäs ja kehittynyt myyntimies, joka tuntee asiakkaan maun, tyylin ja kykenee tekemään älykkäitä päätelmiä ja suosituksia, mitkä suositukset voisivat hyödyttää asiakasta parantamalla mahdollisuutta keskusteluun. Vaikka suosittelijajärjestelmää ensin hyödynnettiin elektronisessa kaupankäynnissä, sitä on kyetty hyödyntämään myös muilla alueilla, erityisesti mediassa. Esimerkkejä onnistuneista suosittelujärjestelmää hyödyntävistä toteutuksista ovat esimerkiksi YouTuben videoiden suosittelu tai Netflix (muut elokuvat, joista saatat pitää). Lisäksi muut teollisuuden alat ovat alkaneet hyödyntää suosittelujärjestelmiä, kuten esimerkiksi liikenneteollisuus. (Naik, 2017)

Nykyään tekoäly on kaikkialla ympärillämme ja suuret yritykset, kuten Google käyttää koneoppimisen menetelmiä suodattaessaan roskapostia Gmail-palvelustaan. Facebook on opettanut tietokoneita tunnistamaan tiettyjä ihmisen kasvojen piirteitä lähes yhtä tarkasti kuin ihmiset tekevät. Netflix ja Amazon käyttävät syväoppimista tekemään päätöksiä siitä, mitä asiakkaat haluavat katsoa tai voivat haluta ostaa seuraavaksi jne. Koneja syväoppimisen menetelmien hyödyntäminen tekoälyn kehittämiseksi on tuottanut lu-

paavia tuloksia ja niiden idea on periaatteessa yksinkertainen. Traditionaalisen tietokoneiden ohjelmoinnin ja älykkääksi tekemisen yrittämisen sijasta tietokoneelle annetaan pääsy laajaan datamäärään ja ne ohjelmoidaan löytämään malleja sekä oppimaan itsenäisesti, miten vaadittu tehtävä suoritetaan. (Buczkowski, 2017)

Terveydenhuollon sektorilla kognitiiviset tietojenkäsittelyjärjestelmät, kuten IBM Watson auttavat lääkäreitä differentiaalisten diagnoosien tekemisessä ja näyttöön perustuvien hoitosuunnitelmien tekemisessä. Pilvipohjaista Big Dataa hyödyntävä tekoäly ja helppokäyttöinen käyttöliittymä, joka kykenee vertaamaan potilaan sairautta koskevaa informaatiota miljooniin anonyymeihin samankaltaisiin diagnosoituihin sairastapauksiin tai taudinkuviin ja maailmalla oleviin lääketieteellisiin tutkimuksiin, auttaa lääkäreitä tekemään oikeita potilaille personoituja hoitosuunnitelmia suhteellisen paljon pienemmällä vaivalla, mikä on aiemmin ollut mahdollista. (Weber, 2015)

Kognitiiviset järjestelmät lisäksi oppivat jatkuvasti ja kehittyvät jopa ”odottaessa”, sillä maailmanlaajuisesti järjestelmiin voidaan syöttää informaatiota jatkuvasti, jolloin järjestelmistä tulee yhä älykkäämpiä ja ne kykenevät diagnosoimaan sairauksia entistä paremmin ja tarjoamaan oikeanlaisia hoitosuosituksia. Tarkoituksena on hyödyntää kognitiivisia tietojenkäsittelyjärjestelmiä lääkäreiden ja muun terveydenhuollon henkilöstön apuna, jotta olisi mahdollista tehdä parempia hoitopäätöksiä tilanteissa, joissa ihmisten kyvyt eivät ole riittäviä. Järjestelmät laajentavat käsittelykykyämme ja tarjoavat mahdollisuuksia laajamittaiselle yhteistyölle.

1.3.1 Neuroverkot

Ihmisen aivojen toimintaa jäljittelevät keinotekoiset neuroverkot keksittiin jo 1940-luvulla. Neuroverkkojen uusi aalto alkoi 1990-luvulla, mutta niiden käyttöinto hiipui nopeasti siihen, että ne eivät olleet muita menetelmiä parempia ja silloisilla tietokoneilla ei ollut mahdollisuutta käsitellä neuroverkkojen koulutuksessa tarvittavia suuria datamääriä. 2010- luvulla koneiden nopeutuminen ja datan määrän valtava kasvaminen ovat kasvattaneet innostusta syväoppimiseen (Deep Learning). Neuroverkkoja käytetään esimerkiksi kuvantunnistuksessa, konenäössä, puheentunnistuksessa, kieltenkääntäjissä, videopeleissä ja lääketieteellisissä diagnooseissa.

Keinotekoiset neuroverkot (Artificial Neural Networks eli ANN) ovat informaation prosessointiparadigma, jota inspiroivat biologiset hermojärjestelmät, kuten aivot. Paradigman avainelementtinä on informaation prosessoinnin järjestelmän uusi malli. Neuroverkot muodostuvat suuresta määrästä toisiinsa yhteen liittyneitä elementtejä (neuronit), jotka toimivat yhdessä tiettyjen määriteltyjen ongelmien ratkaisemiseksi. Keinotekoiset neuroverkot, kuten myös ihmiset, oppivat esimerkeistä. Neuroverkko on voitu esimerkiksi konfiguroida oppimisprosessin kautta jollekin tietylle sovellusalueelle, kuten mallien tunnistaminen tai datan luokittelu. Biologisien järjestelmien oppimiskyky on samankaltainen, sisältäen sovittelua neuronien välisiin synaptisiin yhteyksiin. (Stergiou ym.)

Ensimmäisen neuroverkkotietokoneen kehittäjä, Robert Hecht- Nielsen, määrittelee neuroverkot seuraavalla tavalla:”Neuroverkot ovat tietotekninen järjestelmä, joka on

rakentunut suuresta määrästä toisiinsa kiinteästi liittyneitä prosessointielementtejä, jotka prosessoivat informaatiota dynaamisen tilanvasteen kautta ulkoisille syötteelle”. (Bell, 2014, 91)

Neuroverkkojen vahvuudeksi voisi mainita, että ne voivat ratkaista ei-eksakteja ongelmia epätäydellisillä syötteillä. Neuroverkoilla on kyky oppia vastaanottamiensa syötteiden perusteella uusia ratkaisutapoja, jolloin opittujen ratkaisutapojen myötävaikutuksesta ne voivat ratkaista samankaltaisia ongelmia. Neuroverkoilla on useita erilaisia oppimistapoja, joista yksi tapa on antaa ongelman lisäksi sen ratkaisu, jolloin verkko voi tarkistaa ratkaisun, johon se päätyi omatoimisesti päättelemällä. Toinen mahdollinen tapa on tuoda verkolle sopiva määrä dataa ja antaa sen ratkaista ongelmia itsenäisesti, jolloin oppiminen tapahtuu yrityksen ja erehdyksen kautta. (Bask ym., 1998)

Koneoppimisessa konvoluutioneuroverkot (Convolutional Neural Network eli CNN) ovat tyypiltään monikerroksisia eteenpäin syöttäviä eli Feed Forward keinotekoisia neuroverkkoja, jotka koostuvat yhdestä tai useammasta konvoluutiokerroksesta, joita seuraa yksi tai useampi täysin yhdistynyt kerros standardoidussa monikerroksisessa neuroverkossa. Ne kuitenkin eroavat normaaleista FNN-verkoista siten, että CNN-verkoissa (kuva 18) joidenkin kerroksien neuronit eivät ole kaikkien seuraavien kerroksien neuronien kanssa yhteyksissä. CNN-verkkojen arkkitehtuuri on suunniteltu hyötymään syötteenä lähetetyn kuvan (tai muun 2D-syötteen, kuten puhesignaali) 2D-rakenteesta. CNN-verkot ovat myös helpompia opettaa ja niillä on huomattavasti vähemmän parametreja kuin täysin yhdistyneillä verkoilla, joilla on sama määrä piilotettuja yksiköitä. (UFLDL Tutorial)

Konvoluutioverkot käyttävät hyväkseen konvoluutiokerroksia, jotka suodattavat sisääntulon dataa hyödylliseksi informaatioksi. Näillä konvoluutiokerroksilla on parametreja, jotka on opetettu niin, että ne suodattavat automaattisesti hyödyllisimmän informaation valitun tehtävän suorittamiseksi. Joissain tapauksissa voi olla hyödyllistä suodattaa informaatiota objektin muodosta (objekteilla useimmiten on eri muotoja). Esimerkiksi linnun tunnistamistehtävässä voi olla sopivinta poimia tietoa linnun väristä, sillä useimmilla linnuilla on samankaltainen muoto, mutta ei väritys. Konvoluutioverkot mukautuvat automaattisesti löytämään parhaat ominaisuudet tehtävän suorittamiseksi. (Dettmers, 2015)

Konvoluutioneuroverkot ovat tarjoavat uusinta teknologiaa ja ne voittavat aiemmat menetelmät tarkkuudessa, mutta vaativat huomattavia määriä laskentatehoa ja muistia. Tämä johtaa tilanteeseen, jossa CNN:t toimivat CPU- (Central Prosessing Unit)tai GPU (Graphics Processing Unit)-klustereissa. CCN:iä voidaan hyödyntää kuvien luokittelussa, tunnistamisessa ja lokalisaatiotehtävissä. Tutkimus CCN-verkkojen (ja muiden syväoppimisen teknologioiden) alueella jatkuu nopeana satojen julkaisujen vuosivauhdilla. Ongelmia tosin aiheuttavat valtavat laskentatehon ja muistin vaatimukset, joissa osassa verkkoja voi olla jopa 140 miljoonaa liukulukuparametria ja ne voivat suorittaa yli 15 miljardia liukulukuoperaatiota yhden kuvan luokittelemiseksi. Modernien CNN-verkkojen opetus tehdään lähes aina suurissa CPU- ja GPU-klustereissa. Hyötynä tästä on muun

muassa yhteensopivan syväoppimisen viitekehyksen (kuten Caffe) käyttömahdollisuus. (Zhao ym. 2017)

CNN-neuroverkon opettamisessa on useita eri vaihtoehtoja. Työläin on verkon opettaminen alusta alkaen, jolloin on tarpeen olla suuri määrä dataa, kuten kuvia. Kuvat voivat olla esimerkiksi ajoneuvoista ja CNN-verkko voidaan opettaa tunnistamaan niitä. Mitä enemmän dataa on, sen suurempi on tunnistamisen todennäköisyys. Ongelmana tässä menetelmässä on, että se vaatii huomattavia määriä dataa (esim. kuvia) ja merkittävää laskentakykyä. Toinen vaihtoehto on ns. opitun siirtäminen toiseen tarkoitukseen. CNN-neuroverkko voi olla opetettu esimerkiksi datalla, joka koostuu kissojen ja koirien kuvista. Verkon painoja voidaan hienosäätää ja saada se tunnistamaan esimerkiksi haluttuja auton malleja ja tyyppejä. Tämä menetelmä vaatii huomattavasti vähemmän dataa ja laskentaresursseja. Kolmannessa vaihtoehdossa voidaan käyttää aiemmin opetettua CNN-neuroverkkoa, jonka avulla voidaan hyödyntää sen ominaisuuksia opetettaessa koneoppimisen mallia, kuten tukivektorikone (Support Vector Machine eli SVM), päätöspuu (Decision Tree) jne. Tämä menetelmä vaatii vähiten uutta dataa ja laskennallisia resursseja. (Patel & Pingel, 2017)

1950-luvulla kyettiin mallintamaan neuroverkko, joka oli sienieläimen tasolla ja jossa neuronien lukumäärät olivat vaatimattomia (10^{-2}). Kuluvana vuonna 2017 on kyetty pääsemään mehiläisen tasolle, jossa neuronien lukumäärä on 10^{-6}. Vuoteen 2056 mennessä saatetaan kyetä jäljittelemään ihmisaivojen neuronien lukumäärää (10^{-11}), johon on tosin vielä matkaa. Neuronien välisten yhteyksien määrät ovat myös kasvaneet yli 20-kertaiseksi 50-luvulta nykypäivään. (Goodfellow, 2016, 22)

1.3.2 Koneoppiminen

Koneoppiminen on tekoälyn osa-alue ja data-analyysimetodi, joka automatisoi analyyttista mallin rakentamista. Käyttämällä algoritmeja, jotka iteratiivisesti oppivat käyttämällä dataa, koneoppiminen tarjoaa tietokoneille mahdollisuuden löytää piilossa olevia oivalluksia ja ideoita, vaikkei niiden kohdetta välttämättä edes ollut algoritmiin ohjelmoitu. Koneoppimisessa ohjelmistolle ei aina ole kirjoitettuna algoritmia kaikkia tilanteita varten, vaan kone oppii itsenäisesti ja päätyy haluttuun lopputulokseen. Toiminta on hieman samankaltaista kuin hakukoneilla, jotka tarjoavat niin osuvia- ja oikeita hakutuloksia käyttäjilleen kuin mahdollista. Koneen oppimiskyky kehittyy itsestään aina kun tietoa lisätään tietokantaan. (SAS)

Koneoppimisella on yhteisiä piirteitä tilastotieteen kanssa, sillä molemmissa tehdään päätelmiä aineistoihin perustuen, mutta koneoppimisessa tarkastelun kohteena on ohjelmallisten toteutusten laskennallinen vaativuus. Useat eri päättelyongelmat ovat NP-kovia tai jopa vaikeampia, joten koneoppimisen tutkimiseen kuuluu lisäksi likimääräisten päättelyalgoritmien kehitystyö. Koneoppimisen algoritmit luokitellaan niille annettavan opetusdatan perusteella ja ne ovat:

1. Ohjaamaton oppiminen (opetusdatasta ei tiedetä mitään aiemmin)
2. Ohjattu oppiminen (opetusdatasta tiedetään haluttu ulostulo)
3. Vahvistusoppiminen (oppiminen tapahtuu mallin ja ympäristön jatkuvan vuorovaikutuksen seurauksena)

Ohjatussa oppimisessa konetta opetetaan luokitellun aineiston avulla ja pyritään siihen, että kone osaa tehdä halutun luokittelun samankaltaiselle aineistolle. Klassinen esimerkki ohjatusta oppimisesta on käsinkirjoitettujen numeroiden tunnistus. Ohjaamaton oppiminen jäljittelee ihmisen oppimista. Siinä opettamiseen käytetään raakadataa, josta pyritään löytämään samankaltaisuuksia ja suhteita eri syötteiden välillä, samankaltaiset asiat hakeutuvat toistensa läheisyyteen. Esimerkki ohjaamattomasta oppimisesta on akateemikko Teuvo Kohosen (1934) 1980-luvulla kehittämä itseorganisoituva kartta, jonka sovelluksia on käytetty tuhansissa julkaisussa. Kolmas oppimisen tyyppi on vahvistettu oppiminen, jossa kone oppii ympäristön antaman palautteen perusteella. Käytetään mitä tahansa oppimismenetelmää, niin tekoälystä on hyötyä vasta sitten, kun opettaminen on hoidettu hyvin. (Butcher, 2017)

Koneoppimisessa toteutuvat seuraavat viisi vaihetta (Jain, 2015):

1. **Datan kerääminen**: Data voi olla esimerkiksi raakadataa Excelistä, Accessista tai se voi olla tekstitiedostoista muodostunutta dataa. Datan keräämisen vaihe muodostaa perustan tulevalle oppimiselle. Tärkeää on datan määrä, laatu ja relevanttius.
2. **Datan valmistelu:** Analyyttisten prosessien menestyminen perustuu käytetyn datan laatuun. Aikaa voi kulua datan laadun määrittämiseen ja korjaavien toimenpiteiden suorittamiseen, kuten kadoksissa oleva data tai datassa olevien poikkeavuuksien korjaaminen. Tutkiva analyysi on yksi menetelmistä datan vivahteiden sekä yksityiskohtien tutkimiseen.
3. **Mallin opettaminen:** Tämä vaihe sisältää soveltuvan menetelmän ja datan esitysmuodon valitsemisen mallin muodossa. Käsitelty data jaetaan kahteen osaan, jotka ovat opetus ja testaus. Ensimmäistä osaa käytetään mallin kehittämiseen ja toista osaa käytetään referenssinä.
4. **Mallin arviointi:** Tarkkuuden testaaminen. Datan toista osaa eli testiosaa hyödynnetään mallin arvioinnissa. Tämä vaihe määrittää ulostuloon perustuen menetelmän valinnan tarkkuuden.
5. **Tehokkuuden parantaminen:** Tämä vaihe saattaa sisältää erilaisen mallin valinnan tai muuttujien lisäämisen tehokkuuden parantamiseksi. Tästä johtuen merkittävä määrä aikaa tulee käyttää datan keräämiseen ja valmistelemiseen.

Koneoppimisen kenties tunnetuimpia ohjatun oppimisen malleja ovat päättelypuut (Decision Trees), jotka ovat yksinkertaisia binääripuita, joiden avulla järjestelmä kykenee tekemään päätöksiä. Yksittäiset puut eivät pelkästään ole oppivia järjestelmiä, sillä niiden luonne on staattinen, mutta useiden puiden (metsä) yhteiskäyttö ja uusien puiden luomisen avulla voidaan saavuttaa oppiva järjestelmä. Yksinkertainen päättelypuu voisi kuvata esimerkiksi sitä, lähteekö ihminen aamulla töihin tai kouluun pyörällä. Kulkuväli-

neen valintaan vaikuttavia asioita päätöspuussa ovat matkan pituus, sää ja ihmisen virkeys. Päätöspuun antamaa tulosta voisi esimerkiksi soveltaa bussiaikataulujen lähettämiseen puhelimeen siinä tapauksessa, että pyöräily ei kyseisenä päivänä huvita.

Koneoppimisessa voidaan käyttää myös graafiteoriaan ja todennäköisyyslaskentaan perustuvia malleja, esimerkiksi Bayers-verkkoja. Ne ovat suhteellisen yksinkertaisia, suunnattuja syklittömiä verkkoja, jotka toimivat siten, että jos henkilöllä on koomaan johtava päänsärky, hänellä on todennäköisesti myös aivokasvain. Tämä ei kuitenkaan tarkoita, että tulos on täysin varma eli on mahdollista, että henkilö on kärsinyt päänsärystä ja joutunut koomaan, vaikka hänellä ei ole aivokasvainta. Koneoppimisen yhteydessä Bayers-verkkoja käytetään silloin, jos halutaan kerätä tietoa tuntemattomasta systeemistä, jolloin voidaan aloittaa pienellä verkolla ja lähteä laajentamaan sitä.

Koneoppimista käytetään useilla eri sektoreilla, kuten finanssipalvelut, hallituksien toiminnot, terveydenhuolto, markkinointi ja myynti, öljy- ja kaasuteollisuus, kuljetusala jne. Ehkä kuitenkin tunnetuimpia koneoppimisen käyttötavoista nykypäivänä on mallien tunnistaminen (Pattern Recognition), koska sen avulla voidaan tunnistaa useita eri tyyppisiä kuvia. Esimerkiksi USA:n posti käyttää koneoppimista tunnistamaan käsialakirjoitusta. (SAS; Sarkar, 2016)

1.3.3 Syväoppiminen

Syväoppiminen (Deep Learning) on koneoppimisen osa-alue, joka alkoi kehittyä vuodesta 2006 ja se on tullut pinnalle yhä enemmän vuoden 2012 jälkeen. Kyseisellä osa-alueella käytetään useita epälineaarisia informaation prosessoinnin tasoja ja hierakkisia arkkitehtuureita. Syväoppimisen tavoitteena on luoda sopivaa syväoppimisen algoritmia käyttäen neuroverkkoa, joka tähtää soveltuvan ongelman ratkaisemiseen. Ongelmia, joiden ratkaisemiseen syväoppimista käytetään, ovat perinteisiä menetelmiä käyttäen vaikeita toteuttaa, sillä ne vaativat monimutkaisten sääntöjen käyttöä. Syväoppimisen hyödyntämisen alueita ovat muun muassa lääketieteen diagnostiikka, puhe, kuvat, tekstien tunnistaminen ja käsittely. Monelle tunnetuimpia hyödyntämisen alueita ovat puheentunnistus, kuten Applen Siri ja Googlen Street View-karttapalvelu. (Tjoa, 2013; Jagreet, 2017)

Syväoppiminen Akagin (2014) mukaan:

- On kokoelma tilastollisia koneoppimisen teknologioita
- On toimintahierarkioiden oppimiseen käytetty työkalu
- Perustuu keinotekoisiin neuvoerkkoihin

Syväoppimisen algoritmien suorituskykyä voidaan parantaa muun muassa:

1. Lisäämällä dataa
2. Tuottamalla/generoimalla lisää dataa
3. Dataa uudelleen skaalaamalla
4. Dataa muuntamalla

Syväoppiminen ja lisäksi muut modernit epälineaariset koneoppimisen teknologiat tulevat suorituskykyisemmiksi, mikäli dataa lisätään. Dataa tuottamalla/generoimalla suorituskykyä voidaan myös parantaa ja esimerkiksi kuvadatan ollessa kyseessä, jo olemassa olevien kuvien kääntäminen tai kääntäminen sekä kohinan (Jitter) lisääminen voi parantaa mallin yleistettävyyttä. Datan uudelleen skaalaus on tärkeä vaihe ennen kone- ja syväoppimisen algoritmien käyttämistä. Data-aineistosta voidaan tehdä uudelleen skaalattuja kopioita ja niitä voidaan kilpailuttaa toisiaan vastaan, jolloin on mahdollista nähdä hyödyt ja puutteet datan uudelleen skaalauksesta tietyillä malleilla. Dataa muuntamalla neuroverkot voidaan saada oppimaan nopeammin, jos ratkaistavan ongelman rakenne on paremmin oppivien verkkojen käytössä. (Brownlee, 2016)

Syväoppiminen voidaan nähdä koneoppimisen algoritmien haarana perustuen useiden eri tasojen kykyyn oppia, jotka samanaikaisesti vastaavat useita eri abstraktiotasoja. Tekoäly on ajan saatossa kehittynyt sääntöpohjaisista järjestelmistä koneoppimisen kautta syväoppimiseen saakka. Sääntöpohjaiset järjestelmät ovat soveltuvia ohjelmointialgoritmeja, jotka noudattavat toteutettuja tekoälyohjelmia. Ohjelmien vaatiman tietämyksen tuottavat kyseiseen alaan perehtyneet asiantuntijat, jonka vuoksi sääntöpohjaisia järjestelmiä kutsutaan asiantuntijajärjestelmiksi. Kyseiset järjestelmät sisältävät faktoja ja logiikkaa, jotka yhdistävät faktat kysymyksiin vastaamiseksi. Klassisessa koneoppimisessa syötteenä tulevat ominaisuudet suunnitellaan manuaalisesti ja järjestelmä automaattisesti oppii hyödyntämään niitä ulostuloihin. Tämänkaltainen koneoppiminen toimii hyvin yhden mallin (single pattern) tunnistamisen ongelmissa. Tiedossa on, että käytännössä suurin osa ajasta kuluu optimaalisten ominaisuuksien suunnitteluun. Ominaisuuksien suunnittelun jälkeen voidaan käyttää geneeristä luokittelijaa ulostulon saavuttamiseksi.

Vähäistä esityötä vaativaa ja koneoppimista painottavaa lähestymistapaa kutsutaan representaation oppimiseksi (representation learning). Representaation oppiminen menee yhden askeleen eteenpäin ja eliminoi ominaisuuksien manuaalisen suunnittelun tarpeen. Tärkeimmät ominaisuudet kyetään löytämään datasta automaattisesti. Neuroverkkojen ollessa kyseessä, ominaisuuksia voidaan automaattisesti oppia raakadatasta. Syväoppiminen on myös tietynlaista representaation oppimista, jossa on useita ominaisuustasoja. Nämä ominaisuudet voidaan löytää automaattisesti ja ne kootaan yhteen eri tasoilla ulostuloa varten. Jokainen taso edustaa abstrakteja ominaisuuksia, jotka perustuvat aina aiemman tason ominaisuuksiin. Tällöin abstraktion taso kasvaa aina jokaisella tasolla. Tämänkaltainen oppiminen mahdollistaa korkeamman tason abstraktioiden löytämisen ja hyödyntämisen. Neuroverkoissa useampi taso vastaa useampaa ominaisuustasoa ja nämä useat kerrokset kokoavat ominaisuudet ulostuloa varten. (Goodfellow, 2016)

1.4 Tekoälyn hyödyntämisen alueita

Tekoälyä on hyödynnetty viime vuosina useilla eri alueilla aina terveydenhuollosta sotilaskäyttöön ja älykkääseen infrastruktuuriin saakka. Tekoälyn hyödyntäminen terveydenhuollossa painottuu farmasian, insomnian, kardiologian, onkologian ja pulmonologian alueille. Erityisesti onkologian alueella on toteutettu merkittäviä diagnosoivia tekoälysovelluksia, joiden avulla on kyetty diagnosoimaan muun muassa ihosyöpiä, aivokasvaimia ja rinta- sekä keuhkosyöpiä. Tekoälyllä on myös muita lääketieteellisiä sovellusalueita kuin edellä mainitut kategoriat ja sen avulla voidaan tunnistaa muun muassa silmäsairauksia, kuten kaihia. Sitä voidaan hyödyntää myös mielenterveydellisiin diagnosointeihin, kuten haasteellisen skitsofrenian diagnosointiin.

Terveydenhuollon tulevaisuudesta on ennustettu, että tekoälymarkkinat terveydenhuollon alueella ylittävät kuuden miljardin rajan vuonna 2021. Ala on siis vahvassa kasvussa. Tekoäly tulee muuttamaan terveydenhuollon kenttää tulevaisuudessa kenties huomattavasti ja sen avulla voidaan tehdä tarkempia sekä nopeampia diagnosointeja, löytää uusia lääkeaineyhdistelmiä, tehdä hoitosuosituksia ja säästää kustannuksissa. Tulevaisuudessa sairaalat tulevat olemaan täynnä teknologiaa ja robotiikkaa tullaan hyödyntämään yhä enemmän leikkauksia suoritettaessa ja jatkossa myös logistiikassa, kuten sairaalasänkyjen ja tarvikkeiden automaattiseen kuljetukseen. Sairaalasängyt voivat jatkossa kuljettaa potilasta aina ensiapuhuoneesta operointihuoneeseen saakka ja tarvittaessa kuvantamisen kautta. Tämä auttaa vähentämään henkilöstön tarvetta.

Kognitiiviset tietojenkäsittelyjärjestelmät, kuten IBM Watson auttavat lääkäreitä differentiaalisten diagnoosien tekemisessä ja näyttöön perustuvien hoitosuunnitelmien tekemisessä. Pilvipohjaista Big Dataa hyödyntävä tekoäly ja helppokäyttöinen käyttöliittymä, joka kykenee vertaamaan potilaan sairautta koskevaa informaatiota miljooniin anonyymeihin samankaltaisiin diagnosoituihin sairastapauksiin tai taudinkuviin ja maailmalla oleviin lääketieteellisiin tutkimuksiin, auttaa lääkäreitä tekemään oikeita potilaille personoituja hoitosuunnitelmia suhteellisen paljon pienemmällä vaivalla, mikä on aiemmin ollut mahdollista. (Weber, 2015) Kognitiiviset järjestelmät oppivat jatkuvasti ja kehittyvät jopa ”odottaessa”, sillä maailmanlaajuisesti järjestelmiin voidaan syöttää informaatiota jatkuvasti, jolloin järjestelmistä tulee yhä älykkäämpiä ja ne kykenevät diagnosoimaan sairauksia entistä paremmin ja tarjoamaan oikeanlaisia hoitosuosituksia. Tarkoituksena on hyödyntää kognitiivisia tietojenkäsittelyjärjestelmiä lääkäreiden ja muun terveydenhuollon henkilöstön apuna, jotta olisi mahdollista tehdä parempia hoitopäätöksiä tilanteissa, joissa ihmisten kyvyt eivät ole riittäviä. Järjestelmät laajentavat käsittelykykyämme ja tarjoavat mahdollisuuksia laajamittaiselle yhteistyölle.

Tekoälyä on hyödynnetty ja tullaan hyödyntämään yhä lisääntyvässä määrin myös muilla sovellusalueilla, kuten sotilaskäyttö. Sotilaskäytössä IBM Watsonin tarjoamaa tekoälyä on hyödynnetty Yhdysvaltain Pentagonissa hankintaprosessin toteuttamisessa hyödyntäen luonnollisen kielen prosessointikykyä. Tekoälyn avulla voidaan tunnistaa syöpätapausten lisäksi esimerkiksi maaleja satelliitti- tai tutkakuvista, seulomaan jo olemassa olevaa CV-tietokantaa rekrytointitilanteissa ja analysoimaan, tunnistamaan sekä ennustamaan kyberuhkia. Tekoälyä voidaan käyttää myös taistelukentillä, jossa sitä ollaan

hyödynnetty muun muassa oppimaan ihmisiltä tarkka-ampujan taitoja. Tekoäly yhdistyy hyvin myös robotiikkaan ja Yhdysvallat ovat hyödyntäneet tekoälyn mahdollisuuksia Perdix-lennokeissa, jotka ovat toisiinsa mukautuvia kollektiivisia organismeja, joilla on hajautettu älykkyys päätöksentekoa varten. Ne kykenevät tulevaisuudessa suorittamaan tiedustelutehtäviä ja kohdistettuja hyökkäyksiä. Kyseisenlaisia lennokkeja voidaan hyödyntää puolustushallinnossa valvomaan taistelukenttien muuttuvia tilanteita generoimaan dataa muun muassa tekoälyä hyödyntävien järjestelmien seulottaviksi reaaliaikaisen automaattisen tilannekuvan muodostamiseksi.

2 KYBERTURVALLISUUS

2.1 Mitä kyber ja kyberavaruus tarkoittavat?

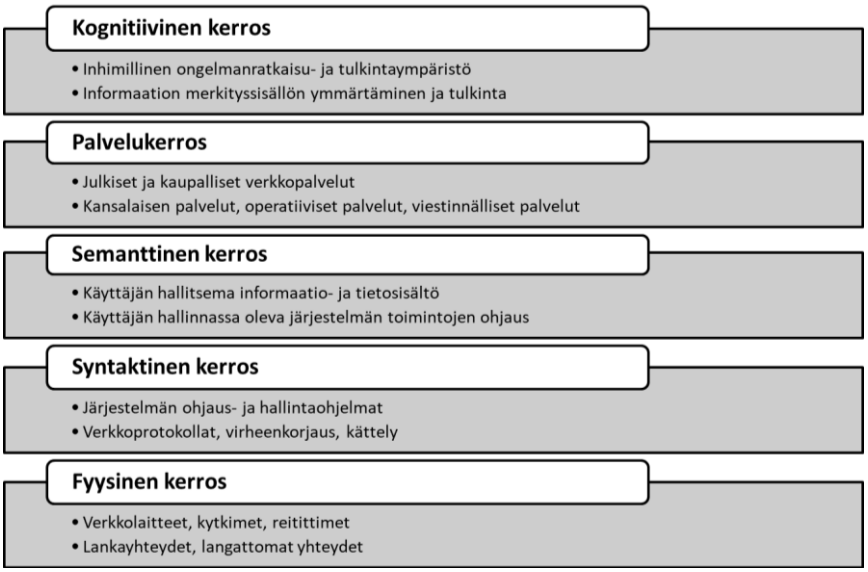
Kyber tarkoittaa ympärillämme olevaa digitaalista biteistä koostuvaa keinotekoista maailmaa, johon kuuluvat muun muassa Internet ja sosiaalinen media, erilaiset tietoverkot- ja järjestelmät, älylaitteiden ohjelmistot jne. Sana kyber tulee kreikankielen sanasta kybereo, joka tarkoittaa ohjaamista, opastamista ja hallitsemista. 1980-luvulla tieteisromaani Neurovelho (Neuromancer) yhdisti kyber- ja space sanat kokonaisuudeksi. Ennen Neurovelhon ilmestymistä kyber määritti tunnettua tutkimusalaa kybernetiikkaa, jonka juuret johtavat Norbert Wienerin vuonna 1948 julkaisemaan Cybernetics: Or Control and Communications in the Animal and the Machine-teokseen. Teoksessa tutkittiin ohjaamisen ja valvonnan (control) suhdetta viestintään. Wiener painotti, että tehokas toiminta vaatii erityisesti viestintää huolimatta siitä, oliko kyse orgaanisen tai mekaanisen järjestelmän ohjaamisesta. (Limnéll ym., 2014, 29)

Wienerin mukaan kybernetiikka käsittelee tieteitä, jotka käsittelevät kommunikaation ja palautteen välityksellä tapahtuvaa koneiden ja elävien organismien valvontaa. Biologisia, fyysisiä ja kemiallisia järjestelmiä voidaan kontrolloida informaatiota jakamalla ja manipuloimalla. Kybernetiikka koskee vain koneiden kaltaisia järjestelmiä, joissa järjestelmän toiminta ja lopputulos voidaan mallintaa ja määrittää matemaattisesti tai ainakin ennustaa. Kyberneettinen järjestelmä on suljettu järjestelmä, joka ei välitä energiaa tai materiaa ympäristönsä kanssa. Kyber-etuliite usein ilmenee tietokoneiden ja robottien yhteydessä ja kybertila (engl. cyberspace) voidaan nähdä tietynlaisena globaalina matriisina, joka on informaatioteknologinen kolmiulotteinen verkosto, johon data on koodattuna erilaisin värein väritettynä ja jossa käyttäjä voi liikkua avatarina esimerkiksi urbaaneissa alueissa. (Lehto ym., 2015, 3)

Kybertila tai kyberavaruus on ihmisen luoma ekosysteemi, joka voidaan nähdä myös hermojärjestelmänä, joka kontrolloi fyysistä maailmaa. Kybertila koostuu sadoista tuhansista toisiinsa yhteydessä olevista tietokoneista, palvelimista, reitittimistä, kytkimistä, valokuitukaapeloinneista ja langattomista verkoista, jotka tekevät infrastruktuurin kehityksen mahdolliseksi. Tämänkaltainen systeemi vaatii jatkuvaa ihmisen läsnäoloa ja aktiviteetteja, jotta se voisi pysyä toimintakykyisenä. Kybertila yhdistää kaikki informaatioteknologiset verkot, tietokannat ja informaatiolähteet yhdeksi globaaliksi virtuaaliseksi järjestelmäksi. Kyberavaruuden rakenteet sisältävät talouden, politiikan, aseelliset voimat, psykologian ja informaation sekä joidenkin tulkintojen mukaan myös yhteiskunnalliset ja infrastruktuurilliset alueet. Juuri informaatiolla on oleellinen rooli kyberuhkatilanteissa ja läntiset informaatioyhteiskunnat ovat siitä riippuvaisia. (Lehto ym., 2015, 4 - 5)

Martin C. Libicki on luonut neliportaisen kybermaailmaan rakenteen, jonka idea perustuu OSI-malliin (Open Systems Interconnection Reference Model). OSI-malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa. Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs. Soveltaen

Libickin kybermaailman mallia on mallinnettu viisikerroksinen hierarkkinen verkostomalli, jonka kerroksia ovat fyysinen, syntaktinen, semanttinen, palvelu ja kognitiivinen (kuva 6). Fyysiseen kerrokseen kuuluvat tiedonsiirtoverkon fyysiset osat, kuten verkkolaitteet, kytkimet, reitittimet sekä kiinteät että langattomat yhteydet. Syntaktinen kerros muodostuu erilaisista järjestelmien ohjaus- ja hallintaohjelmista, liityntäteknologioista sekä toiminnoista, joilla verkkoon kytketyt laitteet ovat vuorovaikutuksessa keskenään, kuten verkkoprotokollat, virheenkorjaus, kättely jne. Semanttinen kerros toimii koko verkon keskuksena ja se sisältää informaatiota sekä aineistoja, jotka sijaitsevat käyttäjien tietokoneilla. Palvelukerros sisältää kaikki julkiset ja kaupalliset palvelut, joita käyttäjä verkossa käyttää. Kognitiivinen kerros kuvastaa käyttäjän informaatiotietoista ympäristöä, maailmaa, jossa informaatiota tulkitaan ja jossa kontekstuaalinen ymmärrys informaatiosta luodaan. Laajemmassa perspektiivissä kognitiivinen kerros voidaan nähdä mentaalisena kerroksena, joka sisältää käyttäjän kongnitiivisuuden sekä tunnetietoisuuden. Kyberavaruus on enemmän kuin vain Internet, joka sisältää laitteistoja, verkostoja ja tietojärjestelmiä sisältäen myös ihmiset sekä sosiaalisen vuorovaikutuksen edellä mainittujen välillä. (Lehto 2014, 75-76)



Kuva 6 Viisi kybermaailman kerrosta (Lehto ym., 2015, 6)

Kyberturvallisuus yleisesti viittaa kykyyn kontrolloida pääsyä verkossa sijaitseviin järjestelmiin ja informaation, joita ne sisältävät. Kyberturvallisuuden kontrollien ollessa tehokkaita, myös kyberavaruutta voidaan pitää varmana, joustavana ja luotettavana digitaalisena infrastruktuurina. Mikäli kyberturvallisuuden kontrollit ovat puutteelliset, epätäydelliset tai heikosti suunnitellut, kyberavaruutta voidaan pitää digitaalisen ajan niin sanottuna villinä läntenä. Kyberturvallisuus jättää tulkinnan varaa, sillä jopa heillä, jotka työskentelevät kyberturvallisuuden parissa, on toisiinsa verrattuna näkemyseroja kyberavaruudesta, jonka kanssa he henkilökohtaisesti ovat tekemisissä. Olkoon systeemi fyysinen palvelu tai kokoelma kyberavaruuden komponentteja, turvallisuusammattilaisen rooli kyseisen järjestelmän suhteen on tehdä suunnitelmia potentiaalisten hyökkäysten ja niistä aiheutuvien seurauksien estämiseksi. (Bayuk ym., 2012)

Kyberturvallisuus viittaa teknologioihin, prosesseihin ja käytänteisiin, jotka on suunniteltu suojelemaan verkkoja, laitteita, ohjelmia, dataa hyökkäyksiltä, vahingoilta tai luvattomalta käytöltä. Kyberturvallisuutta voidaan myös kutsua informaatioteknologian turvallisuudeksi. (Lord, 2017)

Kyberturvallisuus on tietokoneiden ja palvelinten, mobiililaitteiden, elektronisten järjestelmien, verkkojen ja datan turvaamisen käytäntö haitallisia hyökkäyksiä vastaan. Termi on laaja-alainen ja soveltuu kaikkeen tietokoneiden turvallisuudesta katastrofeista toipumiseen ja loppukäyttäjien koulutukseen saakka. (Kaspersky lab, 2018)

Kyberturvallisuus on kokoelma työkaluja, menettelytapoja, turvallisuuskonsepteja, turvatoimia, ohjeistuksia, riskien hallinnan lähestymistapoja, toimintoja, koulutusta, parhaita käytänteitä, vakuutuksia ja teknologioita, joita voidaan hyödyntää kyberympäristön sekä organisaation ja käyttäjän turvaamiseen. Organisaation ja loppukäyttäjän omaisuus käsittää toisiinsa yhteydessä olevia tietoteknisiä laitteita, henkilökuntaa, infrastruktuuria, sovelluksia, palveluita, telekommunikaatiojärjestelmiä ja kaiken lähetetyn sekä tallennetun tiedon kyberympäristössä. Kyberturvallisuus pyrkii varmistamaan organisaation ja käyttäjän varojen turvallisuusominaisuuksien saavuttamisen ja ylläpidon tietoturvariskejä vastaan kyberympäristössä. (ITU, 2018)

Korkealla tasolla kyberturvallisuus selitetään tyypillisesti kolmisanaisina joukkoina, jotka kuvaavat turvallisuusalan ammattilaisten tavoitteita ja heidän metodejaan. Kolme seuraavaa joukkoa kuvaavat kyberturvallisuutta eniten:

- Estää, tunnistaa, vastata (protect, identify, respond)
- Ihmiset, prosessit, teknologia (people, processes, technology)
- Luottamuksellisuus, eheys ja saatavuus (confidentiality, integrity, availability)

Estää, tunnistaa ja vastata-joukon tavoitteet kohdistuvat sekä fyysiseen kerrokseen että kyberturvallisuuteen. Traditionaalisesti primäärinen tavoite turvallisuuden suunnittelussa on ollut estää vastustajan hyökkäyksen menestyminen. Turvallisuusalan ammattilaiset ovat kuitenkin sitä mieltä, ettei kaikkia hyökkäyksiä ole mahdollista estää, joten suunnittelun ja valmistelun tulee sisältää menetelmiä tunnistaa käynnissä olevia hyökkäyksiä mieluiten ennen kuin ne aiheuttavat haittaa. Olivat tunnistusprosessit miten tehokkaita tai tehottomia tahansa, järjestelmän selvästi ollessa hyökkäyksen kohteena, sillä on kyky vastata hyökkäyksiin. Fyysisessä turvallisuudessa termi ”ensimmäiset vastaajat” viittaavat sankarillisiin henkilöihin, kuten palomiehiin, ensiavussa työskenteleviin terveydenhuollon ammattilaisiin tai poliisiin jne. Vastaus hyökkäyksiin tyypillisesti sisältää hyökkäyksien torjumisen esimerkiksi hoitamalla onnettomuuksista eloonjääneitä tai vartioimalla vaurioitunutta varallisuutta. (Bayuk ym. 2012)

Kyberturvallisuudessa edellä mainitun joukon kolmas elementti usein kuvattu optimistisemmin ja vastaamisen sijasta sitä voisi kuvata toipumiseksi tai korjaamiseksi. Toipuminen ja tilanteen korjaaminen voivat olla oikeanlaisia tapoja reagoida hyökkäykseen, sillä informaatioteknologia tarjoaa mahdollisuuden monimuotoisen, uudelleen muodostettavan ja helposti toistettavan datan hyödyntämiseen. Tästä johtuen informaatioturvallisuuden ammattilaiset odottavat, että vika tai vahinko voidaan korjata täydellisesti. Kuitenkin, lopputuloksena saadut tulokset parantavat ennalta ehkäisevää hyökkäyksen torjunnan suunnittelua luomalla iteratiivisen silmukan. (Bayuk ym., 2012)

Ihmiset, prosessit ja teknologia käsittelevät metodeita, jotka ovat yleisiä sekä teknologian hallinnalle yleisesti ja kyberturvallisuuden hallinnalle erikoisalana. Tämä joukko tarkkailee, että järjestelmä vaatii operaattoreita, joiden tulee seurata jo muodostettuja rutiineita, jotta järjestelmä voi suorittaa tehtävänsä. Tämä joukko tähdentää tosiasiaa, että turvallisuutta eivät voi saavuttaa asiantuntijat yksinään ja myös siksi kyberturvallisuutta ei voida saavuttaa vain pelkästään teknologiaa hyödyntämällä. Turvattava järjestelmä tai organisaatio joutuu sisällyttämään suunnitteluunsa muita elementtejä, kuten ihmisten mukanaan tuoma aineeton pääoma, jolla on elintärkeä rooli turvallisuuden suunnittelun ohjelmissa. Vaikka kyseisillä ihmisillä olisi motivaatiota ja kiinnostusta toimia turvallisesti, he eivät yksilöinä tietäisi kuinka kollektiivisesti toimia estääkseen, tunnistaakseen ja toipuakseen hyökkäyksiä aiheutuneista vahingoista ilman ennalta suunniteltua prosessia. Turvallisuusalan ammattilaiset joutuvat tästä johtuen kehittelemään turvallisuusohjelmia organisaatioprosesseihin ja hyödyntämään teknologiaa strategisella tavalla tukeakseen kyberturvallisuuden tavoitteita. (Bayuk ym., 2012)

Luottamuksellisuus, eheys ja saavutettavuus käsittelevät turvallisuustavoitteita, jotka ovat informaatiolle ominaisia. Luottamuksellisuus viittaa järjestelmän kykyyn rajoittaa informaation levitystä oikeutettua käyttöä varten. Eheys viittaa kykyyn säilyttää aitous, tarkkuus sekä tallennetun ja raportoidun informaation alkuperä. Saavutettavuus viittaa oikea-aikaiseen toiminalliseen kykyyn. Näillä informaatioturvallisuuden tavoitteilla oli vaikutusta jo ennen kuin ne olivat tietokoneella, mutta kyberavaruuden ilmestyminen on muuttanut tapoja, joilla tavoitteet saavutetaan sekä niihin liittyvää vaikeustasoa. Teknologiat, joiden on tarkoitus tukea luottamuksellisuutta, eheyttä ja saatavuutta ovat usein ristiriidassa toistensa kanssa. Esimerkiksi pyrkimys saavuttaa korkea informaation saavutettavuus kyberavaruudessa vaikeuttaa informaation luottamuksellisuuden ylläpitämistä. Yleistasolla kyberturvallisuus viittaa metodeihin, joiden avulla voidaan hyödyntää ihmisiä, prosesseja ja teknologiaa, jotta voidaan estää, tunnistaa ja toipua informaation luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuneisiin vahinkoihin. (Bayuk ym., 2012)

2.2 Kyberturvallisuuden kehitys suurtietokoneista Internet-aikaan

2.2.1 Suurtietokoneista henkilökohtaisiin tietokoneisiin

Kyberturvallisuuden historia alkoi 1960-luvulla suurtietokoneiden (engl. mainframe) aikakaudella. Suurtietokoneet olivat ensimmäisiä tietokoneita, jotka olivat riittävän edullisia liiketoiminnan käyttöön ja joita voitiin hyödyntää ROI:n (Return on Investment) laskemiseen investoinneista. Toisen maailmansodan jälkeen vuona 1946 useat yritykset alkoivat työskennellä kaupallisten suurtietokoneiden parissa ja vuonna 1951 UNIVAC-yrityksen kehittämää suurtietokonetta kyettiin hyödyntämään presidentin vaalitulosten ennustamisessa, joka osaltaan auttoi popularisoimaan uutta teknologiaa. Aiemmin sana ”tietokone” viittasi henkilöön, joka suoritti laskutoimituksia ja sana ”kyber” kuului tieteiskirjallisuuden maailmaan. (Bayuk, 2012) 1960-luvulla Yhdysvalloissa käytettiin jo 5000 suurtietokonetta ja niiden määrä nousi nopeasti seuraavalla vuosikymmenellä peräti 80 000 saakka. Kehitys toi uusia eväitä kyberrikollisuuden kehittymiselle. (Brenner, 2010, 10)

Tietokoneilla toteutettu rikollisuus 1960- ja 1970-luvulla erosi nykyajan kyberrikollisuudesta muun muassa siten, ettei silloin ollut vielä Internetiä, eikä suurtietokoneet olleet verkottuneet toistensa kanssa. Suurtietokoneet olivat nimensä mukaisesti kooltaan suuria ja IBM:n suurtietokone maksoi miljoonia dollareita ja tarvitsi tilaa kokonaisen huoneen verran ilmastointeineen. Suurtietokoneiden operointi vaati ryhmän teknikoita ylläpitämään sitä ja huolehtimaan, ettei tietokoneen rakenne hajoaisi, mikäli ilmastointi pettäisi. Tämän ajan tietokoneet käyttivät vielä reikäkortteja ja vasta näppäimistöjen kehittäminen 1970-luvulla paransi tietokoneiden käyttömahdollisuuksia, jolloin niitä voitiin käyttää jo pidemmän matkan päästä. Datan tietoturvallisuuteen tuli myös muutoksia ja tietoturvaa alettiin hoitaa räätälöidyn liiketoimintalogiikan kautta. Käyttäjille luotiin kirjautumisnimet, joihin perustuen voitiin toteuttaa valikoita ja näkymiä, joiden avulla käyttäjät kykenivät suorittamaan työtehtäviä. Tällöin oli mahdollista räätälöidä käyttäjille omat datakentät ja valikot, jotka olivat kaikille erilaisia.

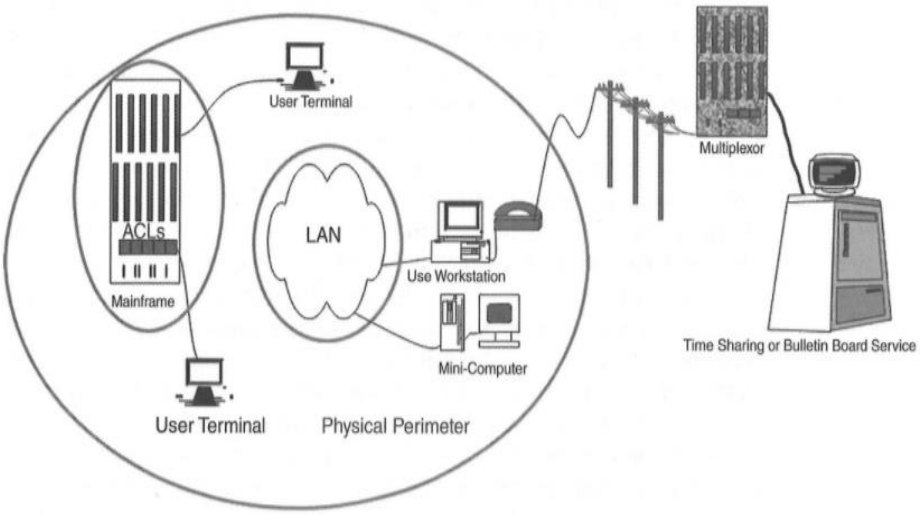
Laajalti levinnyt näppäimistöillä varustettujen tietokoneiden käyttö aiheutti kuitenkin huolia luottamuksellisen valvonnassa, jolloin kehitettiin salausalgoritmeja, jotka muunsivat datan lukukelvottomaan muotoon. Teknologia hyödynsi pitkiä sekvenssejä, joita kutsuttiin avaimiksi ja jotka siten kykenivät salaamaan ja avaamaan datan ymmärtämättömästä takaisin ymmärrettävään muotoon. Tietokoneiden laskentatehon kasvaessa ne pian kykenivät tunnistamaan yhteyksiä viestien ja avaimien välillä. Oli tarpeen alkaa kehittää standardia Yhdysvaltain kansalliseksi salausstandardiksi ja vuoden 1974 U.S. Computer Security Act (Privacy Act) oli ensimmäinen vaihe informaation leviämisen kontrolloinnissa. (Bayuk, 2012, 17)

1970-luvulla minitietokoneet alkoivat saada jalansijaa ja syrjäyttää suurtietokoneita. Minitietokoneet alkoivat nopeasti levitä pienyrityksiin, joilla oli vara hankkia niitä automatisoimaan toimistotehtäviä, kuten tekstinkäsittelyä. Ne yritykset tai tahot, joiden ei ollut vielä mahdollista hankkia omaa minitietokonetta, kykenivät hyödyntämään tarjolla olevaa mahdollista tietokonekäytön aikaperusteiseen hyödyntämiseen (engl. time sharing),

jolloin tietokoneresursseja voitiin käyttää analogisten puhelinlinjojen välityksellä. Yritykset kykenivät näin menetellen hoitamaan verojen sekä palkkojen laskennat ja muita yritykselle oleellisia toimintoja. Nykyään aikaperusteisen ja käyttäjän aktiivisuuteen perustuvien tietokoneresurssien hyödyntämisen on korvannut pilvipalveluteknologia, joka toimii hieman samankaltaisella periaatteella. (Bayuk, 2012, 18)

1970-luvulta 1980-luvulle siirryttäessä Apple ja IBM julkaisivat koti- ja toimistokäyttöön tarkoitetuttuja mikrotietokoneita, joiden tietoturvallisuus pitkälti perustui lukittuihin toimistohuoneisiin. Mikrotietokoneet voitiin yhdistää toisiinsa lähiverkkotekniikalla (LAN eli Local Area Networking), jossa käytetty kaapelointi oli suojattu. LAN-tekniikka vaati keskittimen (enlg. Hub) käyttöä, jotka pidettiin tietoturvallisella alueella. Tietoturvallisuutta parannettiin MAC-kontrolleilla, joiden avulla voitiin nimetä resursseja, kuten ohjelmat ja tiedostot, jotka voitiin yhdistää käyttäjiin, jotka niitä käyttivät. Tietoverkoissa ei kuitenkaan vielä ollut käytössä salausta, vaan kaikki, keillä oli mahdollisuus päästä käsiksi keskittimiin, kykenivät vähällä työllä lukemaan verkossa kulkevia salasanoja. Käytetyt salasanat olivat muutenkin niin heikkoja, että ne olivat pitkälti arvattavissa. (Bayuk, 2012, 19)

Kyberrikollisuutta edesauttoi myös se, että lähiverkko yhdistettiin myös keskustietokoneisiin, jolloin niihin voitiin koettaa murtautua. 1980-luvulla kyberrikollisuus aiheutti uudenlaisia haasteita lainvalvonnalle, joka oli keskittynyt tutkimaan perinteisellä tavalla tehtyjä rikoksia. Jotkut rikollista jäivät kuitenkin kiinni heidän kehuessaan niillä kyseisen ajan sosiaalisen verkoston sivustoilla, jotka olivat pääosin digitaalisia ilmoitustaulupalveluita, joihin voitiin olla yhteydessä analogisia puhelinlinjoja käyttävien modeemien välityksellä. Useat rikolliset jäivät kiinni ja saivat syytteen perustuen dataan, jota löydettiin heidän omilta kotitietokoneiltaan. (Bayuk, 2012, 20) Kuva 7 ilmentää 1980-luvun kyberavaruutta.

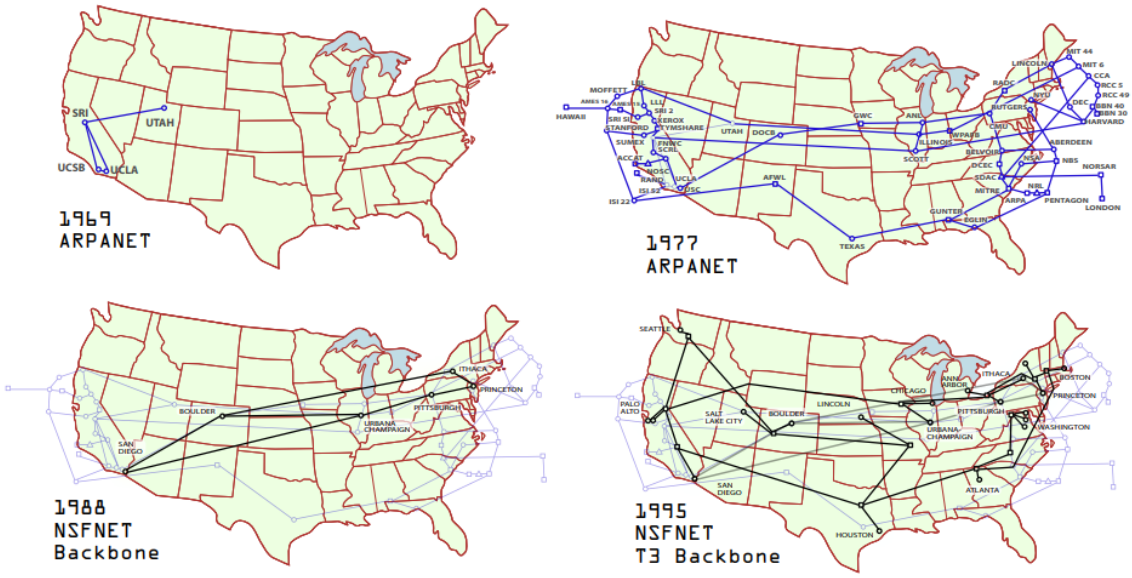


Kuva 7 Kyberavaruus 1980-luvulla (Bayuk, 2016, 20)

2.2.2 Arpanet

ARPANET (Advanced Research Projects Agency Network) (kuva 8) oli Yhdysvaltain sotilaallista tutkimusta varten vuonna 1969 perustettu, vuodesta 1983 lähtien TCP/IP-protokollaa käyttänyt tietoverkko, josta kehittyi Internet. Ensimmäinen viesti Arpanetissä lähetettiin 29. lokakuuta 1969. Tarkoitus oli lähettää UCLA:sta Stanford Research Instituteen (SRI) kirjaimet L, O, G, jolloin UCLA:n kone olisi kirjautunut SRI:n koneelle. Kirjainten L ja O jälkeen Stanfordin kone kuitenkin kaatui.

ARPANET jakaantui kahteen eri verkkoon. Ne olivat MILNET ja ARPANET. ARPANET, joka oli tarkoitettu siviilikäyttöön, levisi yliopistojen ja tutkimuslaitosten välisestä verkostosta huimaa vauhtia nopeasti halventuvan teknologian takia. Siihen liittyi pian runsaasti ulkomaisia solmuja, etenkin Länsi-Euroopasta. Yhdysvaltain puolustuslaitos (DoD eli Department of Defence) toi verkkoinfrastruktuurin useiden tutkimusyliopistojen ja laboratorioiden ulottuville. 1980 –luvulla oli selvää, että tietoverkoilla oli suuri potentiaali akateemisen tutkimuksen apuna, jolloin National Science Foundation kehitti NSFNET –verkon. Yksityinen sektori oli onnistunut alle 10 vuodessa kasvattamaan riittävän Internet-infrastruktuurin, jonka seurauksena ARPANET suljettiin vuonna 1990 ja NFSNET vuonna 1995 Internetin korvatessa ne.



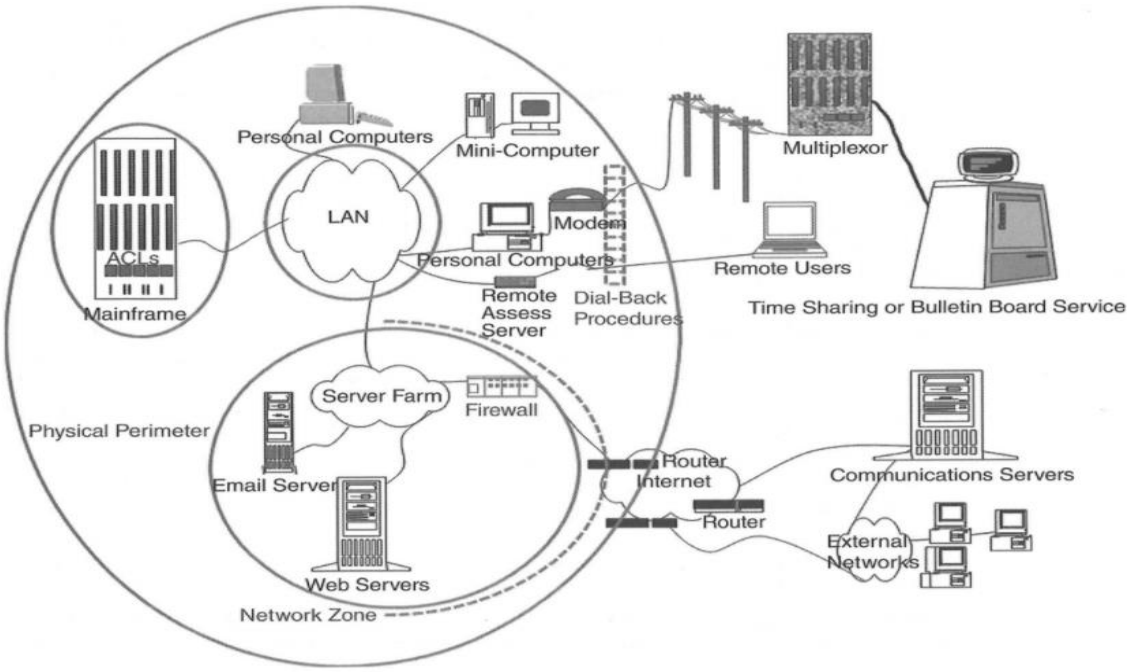
Kuva 8 ARPANET ja NSFNET (Deretsky)

2.2.3 Internet

Kommunikaatio kaupunkien välillä saavutti LAN-verkkojen kypsyystason 1980-luvun loppupuolelle mennessä. Hakemistopalvelut (Directory Services) olivat saatavilla ja mahdollistivat yritysten tietoliikenneyhteydet tutkimus- ja sotilaskäyttöön suunniteltuun ARPANET-tietoverkkoon, joka myöhemmin sulautui julkiseksi Internet-verkoksi. ARPANET-verkossa olleet palvelut vaikuttivat aiemmilta digitaalisilta ilmoitustaulupalveluita, jotka vain olivat yritysten tietokoneilla olevia ja niiden tarjoamia palveluita, joihin voitiin olla yhteydessä modeemien välityksellä. Ainoa huomattavissa oleva ero oli kyky lähettää sähköpostia. Teknologiamyönteiset yritykset nopeasti rekisteröivät domain-nimensä, jotta heillä olisi oma paikkansa kyberavaruudessa. (Bayuk, 2016, 21)

Kyberavaruus oli kuitenkin pian uhattuna, sillä Morris Robert Tappan kehitti ensimmäisen Internet-madon, joka tunnettiin nimellä Morrisin mato. Morrisin mato hyödynsi tietokoneita, joita käytettiin sähköpostipalvelimina hyödyntäen niissä olevia haavoittuvuuksia. Muutamissa tunneissa suurin osa Internetistä oli saastunut ja vahingot olivat suuret, jolloin kommunikaatio Internetissä käytännössä loppui. Mato vei niin paljon laskentaresursseja ja verkon kapasiteettia, ettei niitä ollut juuri järjellä transaktioprosesseihin, jolloin liiketoiminnalliset palvelut häiriintyivät. Ainoastaan AT&T:N Bellin laboratoriot olivat hyökkäykseltä suojassa, sillä he olivat kehittäneet palomuurin, joka salli verkkoon pääsyn vain niille paketeille, joiden lähde ja kohde olivat jo hyväksyttyjen listalla. Analogisille modeemeille ei ollut kehitetty palomuuria vastaavaa teknologiaa, mutta erilaiset puhelinteknologiaa hyödyntävät yhdistelmät, kuten soittajan tunnistus (engl. Caller ID) ja takaisinsoittopalvelu (engl. dial-back) täyttivät vaatimukset. (Bayuk, 2016, 22 - 23)

Organisaatiot sallivat palveluidensa käyttäjien olla yhteydessä tietojärjestelmiinsä modeemien välityksellä, mikä tarjosi käyttäjille tietojärjestelmien kotikäytön mahdollisuuden ja nopeasti kasvavan Internetin käyttämisen, joka vielä koostui pitkälti yliopistoista ja muista tutkimuskeskuksista. Ensimmäiset helppokäyttöiset selaimet tarjosivat mahdollisuuden myös vähemmän teknisille ihmisille käyttää Internetiä. Pienistä palvelimista tuli yhä halvempia ja se sai useat yritykset hankkimaan palvelinfarmeja, jotka tarjosivat laajemmat hyödynnettävät resurssit. Lisäksi yritykset kiinnostuivat rakentamaan sähköpostipalvelinten lisäksi myös Web-palvelimia. (Bayuk, 2016, 23) Kuva 9 havainnollistaa, miten edellä mainitut tietokone- ja verkkoresurssit olivat tyypillisesti yhteydessä toisiinsa 1990-luvun alkupuolella. (Bayuk, 2016, 20)



Kuva 9 Kyberavaruus 1980-luvulla (Bayuk, 2016, 24)

1990-luvun alun verkkojen kontrollit eivät kuitenkaan kyenneet estämään hakkereita ja muita tietokoneresursseja laittomasti hyödyntäviä aiheuttamaan haittaa virusten avulla. Kyseisenä aikana viruksia levitettiin levykkeinä (enlg. Floppy Disks). Kyberverkkorikollisuutta tutkivat henkilöt kykenivät kuitenkin analysoimaan virustyyppejä ja luomaan niistä digitaalisen allekirjoituksen tarkastellen jokaista tiedostoa, jota virukset olivat muuttaneet. Tähän perustuen voitiin kehittää Antivirus-ohjelmistoja, eli viruksentorjuntaohjelmia, joita tultiin asentamaan työasemille virusten torjumiseksi. (Bayuk, 2016, 23)

1990-luvun puolivälissä sähköinen kaupankäynti sai vauhtia ohjelmistojen kehittyessä ja Internetin levitessä. Sähköisen liiketoiminnan ohjelmistot ja sivustot korvasivat verkossa olevia esitteitä ja sallivat käyttäjien hankkia tuotteita ja toteuttaa erilaisia taloudellisia transaktioita verkon välityksellä. Tämä kuitenkin avasi hakkereille uusia mahdollisuuksia ja portin 80-haavoittuvuusongelmasta tuli laajalti hyödynnetty tapa päästä sisälle Web-palveluresursseihin. Internetissä käytetty HTTP-protokolla hyödyntää oletuksena porttia 80, jolloin se jouduttiin avaamaan liikenteelle palomuureissa. Web-palvelimet oli suunniteltu siten, että ne hyväksyivät käyttäjien käskyt sisällön näyttämiseksi, mutta myös sallivat käskyt, jotka käskivät niitä hyväksymään ja suorittamaan ohjelmia, joita käyttäjät halusivat. (Bayuk, 2016, 25)

DMZ (Demilitarized Zone) verkkoarkkitehtuurista tuli uusi turvallisuusstandardi, jonka kehitti Bell Labsin tutkijat, jotka olivat luoneet ensimmäisen palomuurin. DMZ on verkkoalue, joka salli pääsyn Internetistä ennalta määriteltyyn joukkoon palveluita. DMZ sijaitsee yrityksen sisäisen verkon (engl. intranet) ja Internetin välissä ja sinne sijoitetaan

yleensä julkisia palvelimia. DMZ-verkkoalueen tehtävänä on estää pääsy yrityksen intranet-verkkoon julkisen verkon kautta. Lähiverkossa turvattomimpia laitteita ovat ne, jotka palvelevat verkon ulkopuolisia käyttäjiä, kuten esimerkiksi sähköposti ja DNS-palvelimet (DNS eli Domain Name System). Nämä laitteet sijoitetaan omaan aliverkkoon, jolloin muu verkko on suojattuna, mikäli hyökkäys palvelimiin onnistuu. DMZ-alueella olevat laitteet eivät kykene suoraan muodostamaan yhteyksiä lähiverkon laitteisiin, mutta muihin saman alueen laitteisiin ja ulkopuolisiin käyttäjiin. DMZ-alueella olevat laitteet kykenevät palvelemaan sisäisiä ja ulkoisia käyttäjiä lähiverkon vaarantumatta. (Bayuk, 2016, 25)

DMZ-alueen ollessa kyseessä Internetistä tuleva liikenne voidaan suodattaa siten, että paketeilla on pääsy ainoastaan palvelimiin, jotka ovat tarkoituksella asennettu julkista käyttöä varten ja joiden tietoturvaa on vahvistettu oletettuja hyökkäyksiä vastaan. Standardiksi käytänteeksi tuona aikana tuli menettelytapa, jossa pääsyn sisäiseen verkkoon kykeni avaamaan vain koko DMZ-alueen tietoturvakontrolleista vastaava tietoturva-arkkitehti. Tietoturvakontrollien testaaminen ennen palvelinten käyttöönottoa kehittyi tietoturvatarkastusten integroimiseksi järjestelmäkehityksen elinkaareen. Menettelytavasta tuli lopulta kansainvälinen standardi (ISO/IEC 2002, 2009C). (Bayuk, 2016, 26)

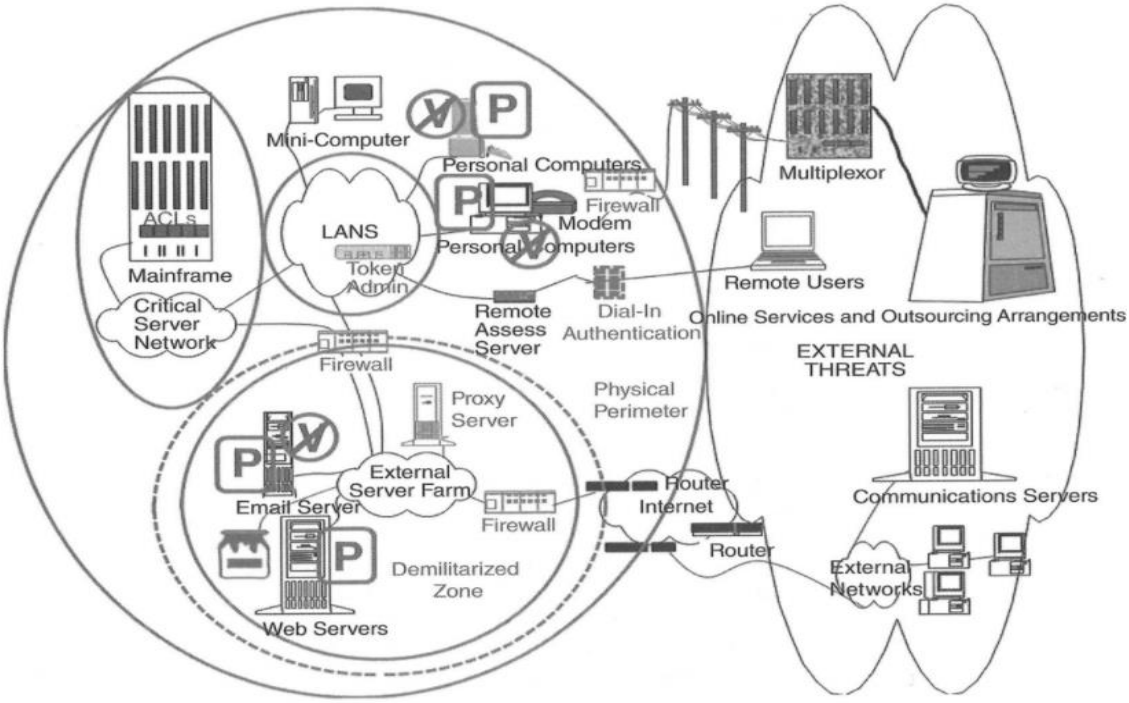
Palvelinten etäkäyttäjien lukumäärän kasvu pahensi virusongelmaa, joka oli lähtenyt kasvuun 1990-luvulla. Virustorjuntaohjelmistojen ja työasemapäivitysten lisäksi useiden erilaisten yritysten oli alettava tekemään yhteistyötä tietoturvaohjelmistoja tuottavien yritysten kanssa saadakseen tilannekuvan siitä, miten virukset olivat levinneet WWW-sivuilla ja siten kykenivät estämään kyseisten saastuneiden sivustojen käytön sekä estämään viruksia leviämästä sisäiseen verkkoon. Kirjallisuudessa mustien listojen (engl. black lists) käsite tuli myös tutuksi ja niiden tehtävänä oli estää haitallisten ohjelmistojen (engl. malware) leviämistä. Teknologiat, kuten WWW Proxy-palvelimet estivät käyttäjiä pääsemästä mustissa listoissa luetelluille sivustoille. Proxyjen tehtävänä oli tarkastella liikennettä ja verrata sitä organisaation määrittelemiin kommunikaatiosääntöihin. Mikäli liikenteen ja kommunikaatiosääntöjen välillä oli konflikti, liikenteen välittäminen eteenpäin katkaistiin. Toimivan tietoturvan ylläpitäminen vaati jatkuvaa virustietokannan ja proxykonfiguraatioiden ylläpitämistä sekä päivitysten asentamista. (Bayuk, 2016, 27)

Kuva 10 havainnollistaa tyypillistä 1990-luvun puolivälin verkkotopologiaa, tosin huomattavasti yksinkertaistettuna. Kuvassa yliviivatut V-kirjaimet indikoivat asennettuja antivirus-sovelluksia ja P:t viittaavat päivityksiin, joita täytyy säännöllisin väliajoin asentaa verkkoon liittyviin tietokoneisiin. Katkoviivoilla kuvataan laitteistoja, joita tyypillisesti löytyy DMZ-verkoista. Tyypillistä oli, että jopa suhteellisen pienillä organisaatioilla saattoi olla satoja PC-tietokoneita ja tusinoittain palvelimia, joiden tietoturva oli hyvin haastavaa hallita. Virustorjuntaan erikoistuneet yritykset toimittivat virustorjunnan hallinnan palvelinohjelmia, jotka kykenivät käymään läpi jokaisen yrityksen intranetissä olevan tietokoneen ja varmistamaan, että tietoturva oli ajan tasalla. Tilanne ei ollut mieliyttävä, mutta kontrolloitavissa.

Mahdollistaakseen asiakasviestinnän salauksen, web-ohjelmistokehitykseen erikoistunut yritys kehitti uudenlaisen salatun viestiprotokollan SSL:n (Secure Socket Layer) vuonna 1995. Vuonna 1999 protokollaa laajennettiin ja sitä alettiin kutsua TSL-protokollaksi (Transport Layer Security). TSL on ollut standardi salattu kommunikaatiomekanismi siitä lähtien. Yleisin TLS-protokollan sovelluskohde on HTTPS-protokolla (Hypertext Transfer Protocol Secure), jota käytetään, kun halutaan salata käyttäjän ja palvelun välinen liikenne. Yleisiä käyttökohteita ovat esimerkiksi verkkokaupat ja pankit sekä selaimella käytettävät sähköpostipalvelut.

Vuonna 2011 tutkijat havaitsivat TSL-salauksessa haavoittuvuuden, jota voitiin hyödyntää BEAST-menetelmäksi tunnetulla tietoturvahyökkäyksellä. BEAST-menetelmässä hyökkääjä ujuttua TSL-salausta hyödyntävään HTTPS-liikenteeseen huomattavasti hyökkääjän itsensä muodostamaa liikennettä. BEAST mahdollistaa esimerkiksi käyttäjän istuntotunnisteen (ns. Sesson ID Cookie) varastamisen. Varastetun tunnisteen avulla hyökkääjä kykenee käyttämään hyväksi suojatussa palvelussa käyttäjän identiteettiä. Käyttäjä ei itse havaitse onnistunutta hyökkäystä. BEAST-hyökkäyksen onnistuminen edellyttää, että hyökkääjä pystyy kuuntelemaan ja muokkaamaan uhrin verkkoliikennettä. Tämänkaltaisen hyökkäyksen toteutus on helpompaa WLAN-verkoissa ja muissa avoimissa suojaamattomissa verkoissa. Hyökkäyksen onnistumiseksi käyttäjän täytyisi geeroida suhteellisen suuria määriä liikennettä, johon kuluu sekä aikaa että verkon kapasiteettia. Salauksen osittainen purkaminen vaatii arvioiden mukaan 10 – 30 minuuttia ja lisäksi verkkoselaimen Same Origin Policyn (SOP) kiertämistä, esimerkiksi Cross Site Scripting (XSS)-haavoittuvuutta hyödyntäen. (Viestintävirasto, 2011)

1990-luvun loppupuolella Internet-yhteydet nopeutuivat huomattavasti ja se tarjosi yritysten henkilöstöille, kuten tavallisille loppukäyttäjille, mahdollisuuden aiempaa kattavampaan informaation hyödyntämiseen. Asiakasdataa käsittelevä yritysten henkilöstö tarvitsi pääsyn yritysten intranetiin, jonka tietoturvallinen hyödyntäminen vaati molemminpuolisen autentikoinnin. Asiakasdatan luottamuksellisena pitäminen vaati koko etäyhteyden salaamisen, jolloin virtuaalinen erillisverkko eli VPN (Virtual Private Network) –teknologia kehitettiin. VPN on tapa, jonka avulla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon. VPN-verkon tietoturva hoidetaan joko salauksella tai fyysisesti. VPN-teknologian määritelmää on sittemmin laajennettu kattamaan myös yksittäisten työasemien liittämisen yrityksen verkkoon. (Bayuk, 2016, 30 - 31)

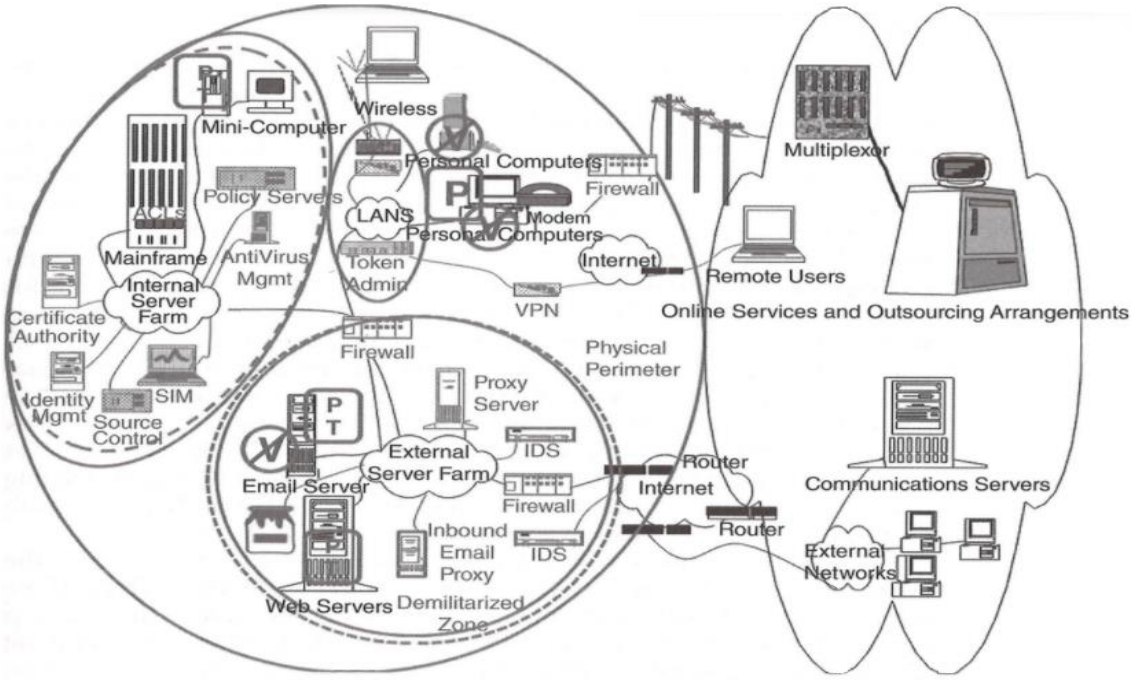


Kuva 10 Kyberavaruus 1990-luvun puolivälissä (Bayuk, 2016, 28)

Tietoverkkojen tietoturvan haasteet kovenivat 2000-luvun alussa, jolloin langattomat yhteydet alkoivat voimakkaasti lisääntyä. VPN-teknologia ja langattomien laitteiden suojaustunnukset eivät kuitenkaan ollet yleistyneet langattomien laitteiden keskuudessa, ennen kuin tutkijat esittivät, kuinka helposti sisäänrakennettu langattomien laitteiden tietoturva oli murrettavissa. Yritysten omaksuessa tai ottaessa uudelleen käyttöön tietoturvateknolioita uudella alueella yrityksen verkossa, oli tarpeen asentaa ohjelmisto tai palvelin, joka tuki tätä tarkoitusta. Palomuurien säännöstöjen, tietoturvapäivityksien, langattomien tietoturva-asetuksien, välityspalvelimien (Proxy) jne. tekniset konfiguraatiot tunnettiin tietoturvapolitiikkana (Security Policy). Oli tarpeen asentaa palvelimia hoitamaan laitteiden tietoturvapolitiikkaa ja pitää kirjaa niiden konfiguraatiomuuttujista, sillä laitteen toimiessa huonosti tai hajotessa oli vaikea luoda uudelleen laitteiden tietoturvapolitiikka. (Bayuk, 2016, 32)

Huolimatta siitä, että tietoturvapolitiikkaa toteutettiin, tietoturvahäiriöitä syntyi silti. Havaittiin, etteivät tietoturvalaitteistot noudattaneet vaadittavaa teknologian konfiguroinnin politiikkaa. Tietoturvapäälliköt joutuivat etsimään perimmäisen syyn, josta tilanne johtui ja tarkastelemaan käyttäjien lokitietoja, joita oli tallentuneena useiden eri laitteiden muisteihin. Tilanteeseen toivat helpotusta SIM (Security Information Management) -palvelimet, jotka suunniteltiin tallentamaan suuria määriä aktiviteettilokitiedostoja ja joihin suuntautui valtava määrä kyselyitä. Kyselyt olivat ennalta suunniteltuja koskien tilanteita, jotka saattoivat indikoida järjestelmään suuntautuvia hyökkäyksiä. (Bayuk, 2016, 32)

Kuva 11 kuvaa tilannetta 2000-luvun alussa. Kuvassa havainnollistuu tietoturvayritysten kehittämät tietoturvaratkaisut, joita on kuvattu harmailla laatikoilla. Tärkeänä komponenttina on myös IDS (Intrusion Detection System), joka tarjosin tietoverkon tasolla olevan hyökkäyksen tunnistamisen järjestelmän. Ideana oli vapauttaa käyttäjät ja heidän työasemansaan virusten tarkastusten haasteista. Tämänkaltainen järjestelmä lisäksi tarjosi enemmän informaatiota siitä, missä Internetissä virus on saanut alkunsa. IDS kykeni myös tunnistamaan DDOS-hyökkäyksiä ja identifioimaan hyökkääjän aiempia aktiviteetteja. (Bayuk, 2016, 28, 33)



Kuva 11 Kyberavaruus 2000-luvun alussa (Bayuk, 2016, 33)

Huolimatta aiemmista tietoturvainnovaatioista, kyberhyökkäykset jatkoivat onnistumistaan. Harmittomilta näyttävät finanssialan toimijoilta tulleet sähköpostit saattoivat sisältää linkkejä sivustoille, joille oli asennettu haittaohjelmia, jotka kysyivät käyttäjän salasanaa tai niiltä saattoi vahingossa ladata tietoturvauhkia aiheuttavia haittaohjelmia. Kyberrikolliset hyödynsivät oikeilta ja turvallisilta sivuilta vaikuttavia sivustoja, jotka ohjasivat varomattomat käyttäjät sivustoille, joiden kautta hyökkääjät kykenivät hyödyntämään tietoturva-aukkoja ja murtautumaan tietojärjestelmiin. Hyökkäyksiä kutsuttiin reaalitodellisuuden esikuviensa mukaan kalastelu- ja farming-hyökkäyksiksi. Kalastelu-hyökkäykset kuvaavat nimensä mukaisesti tilanteita, joissa heitetään kalastuskoukku mereen ja odotellaan, syökö kala. Farming-hyökkäyksissä on kyse ikään kuin siemenen istuttamisesta satoa varten, joka kybermaailmassa tarkoittaa siementen istuttamista myöhempiä hyökkäyksiä varten. Haittaohjelmat voivat kerätä esimerkiksi nimiä ja salasanoja, jotka lähetetään edelleen hämäräperäisille sivustoille, joiden kautta saatua informaatiota voidaan hyödyntää tulevissa kyberhyökkäyksissä. (Bayuk, 2016, 33)

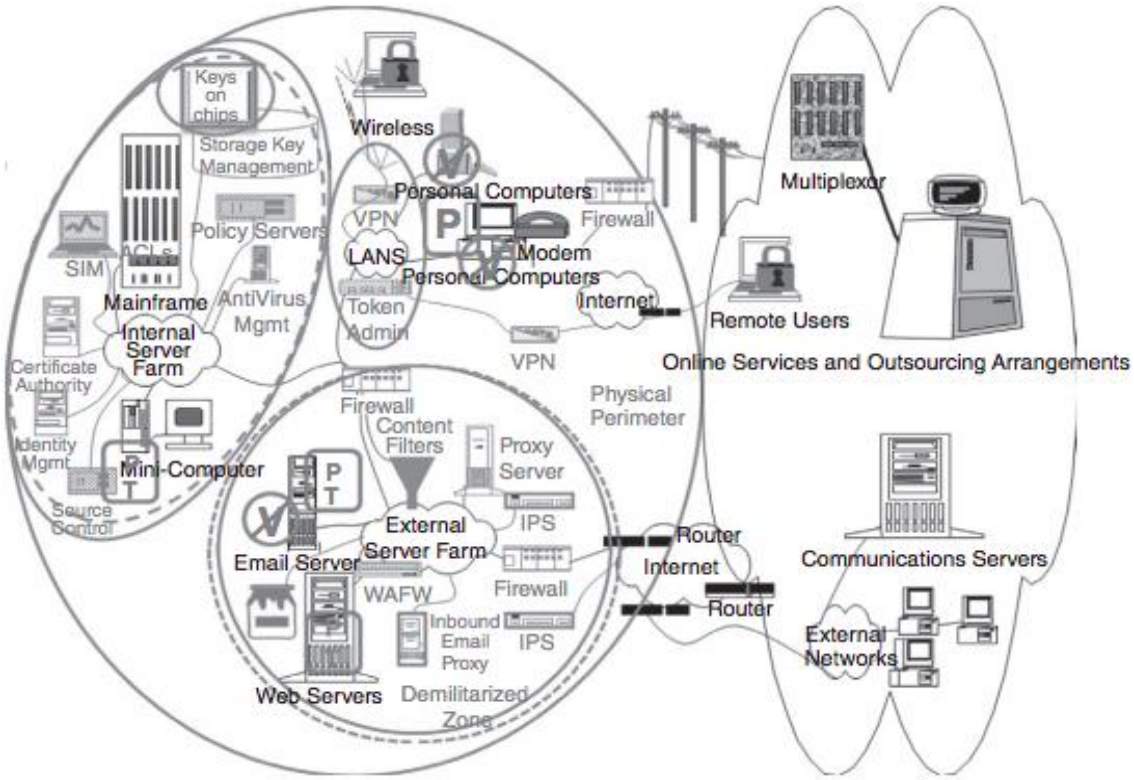
2000 -luvun puolivälissä nähtiin myös huomattavaa organisoidun Internet-rikollisuuden kasvua ja identiteettivarkaudet rehoittivat. Kannettavia tietokoneita ja tallennusväli-

neitä varastettiin, joiden avulla hyökkääjät saivat käsiinsä informaatiota identiteettivarkauksien toteuttamista varten. Käyttäjillä oli myös usein tapana kuljettaa kannettavia massamuisteja sekä kannettavia tietokoneita mukanaan, joka aiheutti tietoturvauhkia. Valmistajat alkoivat nopeassa tahdissa kehittää metodeja, joita hyödyntäen oli mahdollista salata sekä data että sen siirrossa käytetyt USB-muistit. Joskus oli tarpeen myös fyysisesti poistaa kannettavan tietokoneen dvd-aseman tai estää USB-porttien käyttämisen. (Bayuk, 2016, 34)

Tallennusmedian tai datakeskuksen ollessa kyseessä, resurssin, varkaudet yleistyivät ja laitevalmistajien salatessa medioita, salausavainten suojaamisesta tuli vaikeaa. Yksinkertaisia salausavainten hallintajärjestelmiä on ollut olemassa jo 1990 –luvulta saakka. Teknologisten operaatioiden, kuten tuhottujen tiedostojen palauttaminen, vaati oman avaimensa, jolloin avainten tarve kasvoi nopeasti. Oli tarpeen luoda varasto, johon avaimet automaattisesti tallennettiin ja josta niitä kyettiin tarpeen mukaan ottaa käyttöön. Usein avaimia tallennettiin niitä varten kehitetyille siruille, jotka pidettiin eristyksissä ja mikäli itse käytettävä laite varastettiin ilman sirua, tallennusmediaa ei kyetty saamaan purettua luettavaan muotoon. Prosessi aiheutti kuitenkin tilanteen, jossa käyttäjät alkoivat lähettää tiedostoja itselleen sähköpostitse, jotta vaikeasti hyödynnettävät tietoturvakontrollit voitiin välttää. Sähköpostien turvallisuus ei kuitenkaan ollut toivotulla tasolla, vaan siinä oli tunnettuja haavoittuvuuksia. Protokollat, jotka palvelimet hyödyntävät kommunikaatioon ja informaation jakamiseen eivät vielä nykyäänkään ole salattuja ilman erillistä molemminpuolisia sopimuksia. (Bayuk, 2016, 34 - 35)

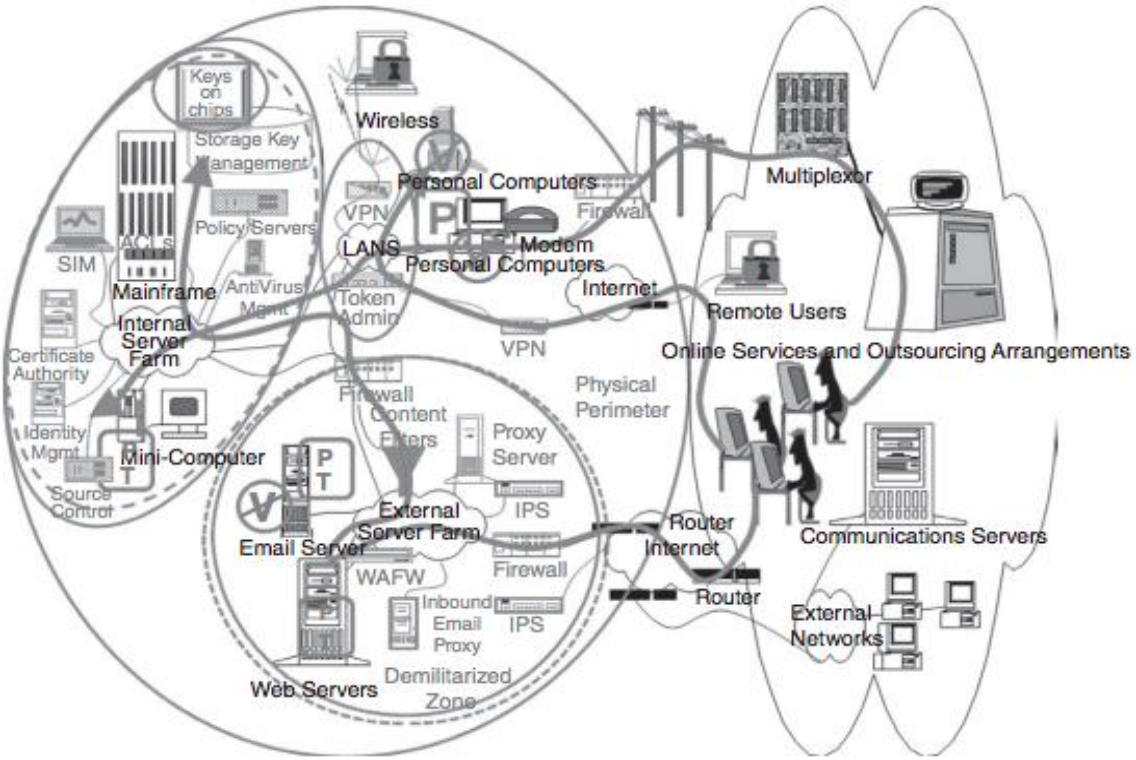
Hyökkääjillä on yhä kyky löytää hyödynnettäviä tietoturva-aukkoja verkkolaitteista, eivätkä kyberhyökkäykset ole vähentyneet. Demilitarisoitu alue (Demilitarized zone eli DMZ) ei kykene estämään web-kehittäjiä tuottamaan ohjelmakoodia, jota voidaan käyttää jäljittelemään verkon toimintaa, jonka web-palvelin mahdollistaa ja sallii. Tämä mahdollistaa pääsyn sensitiiviseen asiakasdataan, jolla voi olla kriittisiä vaikutuksia. Ohjelmistokehittäjät voivat innovoida jakamalla ohjelmakoodia julkisen (open source) tai yksityisomisteisen ohjelmistokehitysprojektin kautta. Projektin alkuvaiheessa ohjelmistokehittäjät tyypillisesti koettavat hyödyntää niin paljon jo luotua ohjelmakoodia kuin mahdollista, jotta he voivat minimoida työmäärän uusien toiminnallisuuksien toteuttamiseksi. Usein nämä ohjelmakoodit sisältävät paljon ohjelmointivirheitä ja vikoja. Ohjelmakoodin sekaan on voitu sisällyttää tietoturvavirheitä. Kyberturvallisuusratkaisujen toimittajat ovat kehittäneet lähdekoodien analytiikkaohjelmistoja, jotka pyrkivät löytämään ohjelmakoodiin sisällytettyjä tietoturva-aukkoja, jotta ne voidaan saada eliminoitua ennen ohjelmiston käyttöönottoa. Kyseiset toimittajat ovat kehittäneet myös järjestelmiä (esim. Web Access Firewall, WAFS), jotka tarkkailevat verkkoliikennettä, jonka kohteena on web-palvelinohjelmisto ja web-palvelimen generoima vastaus. Tämänkaltaiset järjestelmät on ohjelmoitu tunnistamaan suojaamattomia ohjelmistoja, jolloin niiden hyödyntäminen voidaan estää. (Bayuk, 2016, 36)

Kuviosta 12 ilmenee, että salausmekanismit on sisällytetty sekä kriittisiin palvelimiin että etälaitteisiin. Sisältösuodattimet estävät käyttäjiä lähettämästä sensitiivistä informaatiota Internetiin. Tunkeutumisen estolaitteet ovat korvanneet tunkeutumisen tunnistukseen kehitetyt laitteet.



Kuva 12 Kyberavaruus ja kyberturvallisuuden vastatoimet (Bayuk, 2016, 36)

Kyberhyökkäykset eivät ole vähentyneet, vaan päinvastoin ne jatkuvat. Kyberturvallisuuden termi tosin on muotoutunut ajan saatossa tietokoneiden tietoturvasta informaatioturvallisuuteen ja edelleen kyberturvallisuuteen saakka. Kyberuhat eivät ole kadonneet, näin ollen kaikkia vastatoimia voidaan edelleen pitää parhaina käytänteinä. Kuva 13 havainnollistaa polkua, jota nykypäivän kyberhyökkääjät käyttävät. Kyseinen polku on samanlainen, jota kybeturvallisuuteen erikoistuneet insinöörit ovat luoneet mahdollistamaan käyttäjien oikeutetun pääsyn järjestelmään. Oikein ja hyvin toteutettuna kyberturvallisuusratkaisut kykenevät vähentämään hyökkäyksien onnistumisia ja suurimpia uhkia aiheuttavat vakoilu ja paatuneet rikolliset. (Bayuk, 2016, 36)



Kuva 13 Kyberavaruuden hyökkäyspolkuja (Bayuk, 2016, 37)

2.3 Uhat, riskit ja haavoittuvuudet

2.3.1 Kyberuhat

Uhka koetaan ainakin periaatteessa pakottavana toimintana, jossa tavoitteena on aiheuttaa negatiivista vaikutusta kohteessa ja/tai kohteen intresseissä. Kohde pyritään saamaan toimimaan uhkaajan haluamalla tavalla. Uhkaaja koettaa tehdä uhkauksen kohteena olevan toimintavaihtoehdoista rajallisempia eli niitä pyritään minimoimaan. Oleellinen osa uhkaamista on uhkan kertominen (ja toistaminen tarvittaessa) kohteelle, joka voi saada uhkauksen kohteena olevan toimimaan uhkaajan hyväksi. Kyberuhat muodostavat samankaltaisen uhkan kentän kuin muut reaalimaailman uhat, joihin olemme jo sinänsä tottuneet. Uhkan vakavuutta ja uskottavuutta säätelevät arviot uhkaajan kyvyistä, jotka voivat olla materiaalisia tai taitoihin liittyviä. Lisäksi uhkaajan haluun tehdä uhattuna olevalle ilmoitettu toimi ja kohteen riippuvuus omaisuudesta tai toiminnoista, joita kohtaan uhka asetetaan, vaikuttavat. Uhka siten koostuu niin uhkan todellisuudesta kuin uskomuksistakin. (Limnéll, 2014, 105 - 106)

Uhka ei kuitenkaan välttämättä johdu aina suoraan toimijasta, vaan se voi olla abstraktimpi, kuten kyberuhat ovat. Kohdistamattomat ja abstraktit uhat useimmiten ovat hankalasti arvioitavissa järkiperäisesti, jolloin julkinen kohu yleensä ympäröi ne. Tuntematonta uhkakuvaa, jota ei välttämättä ymmärrä, on helppo liioitella. Liioittelu usein kasvaa kohtuuttomaksi ja negatiiviseen suuntaan, jolloin esimerkiksi kyberin kohdalla siinä

ylikorostuu sodankäynti- ja terrorismi. Uhka, jota ei ymmärrä, on erittäin helposti liioiteltavissa. Kybermaailmassa niin kuin fyysisessäkin on hyväksyttävä, ettei kaikkia uhkia voida torjua tai niiltä suojautua. Siten täydellistä kyberturvallisuutta ei ole olemassa, on vain pyrittävä riittävän hyvään tasoon. (Limnéll, 2014, 106)

Tärkeää on, että uhkiin varaudutaan ja niiden negatiivisilta vaikutuksilta koetetaan suojautua. Kyberuhkia kohtaan voidaan parhaiten varautua parantamalla kyberturvallisuuden perusasioita, lisäämällä kaikkien tietoisuutta uhkista, parantamalla toimintakykyä ja ylläpitämällä tietoturvaa. Oleellista on tunnistaa kyberturvallisuuden haasteet ja kyetä reagoimaan niihin asianmukaisesti. Tärkeänä osana kyberturvallisuutta on kyetä pitämään toimintakykyä yllä kyberhyökkäyksen tapahtuessa sekä kyetä päättämään hyökkäys mahdollisimman nopeasti ja lisäksi palauttaa organisaation toiminnot normaaliin tilaan. Tähän tarvitaan myös oikeanlaista lainsäädäntöä ja keskusteluja onkin paljon käyty siitä, minkälaisia vastatoimia kyberhyökkäyksiä vastaan hyökkäyksen kohteena voi laillisesti hyödyntää. (Limnéll, 2014, 107)

Kyberuhkat voivat tulla organisaation ulko- tai sisäpuolelta. Sisäiset uhkat vaikuttavat talouteen, maineeseen ja tietopääomaan. Niiden lähteitä voivat olla tyytymättömät (entiset tai nykyiset) työntekijät, tyytymättömät kumppanit, alihankkijat tai näiden työntekijät. Sisäpiirissä olevilla ei tarvitse olla erityisen syvällistä osaamista informaatioteknologiasta, siihen liittyvistä järjestelmistä tai verkkoon tunkeutumisesta, vaan heillä usein on riittävällä tasolla olevat käyttöoikeudet tai he kykenevät hankkimaan sellaiset kohdetta vahingoittaakseen tai tietoa varastaakseen. Tällaisessa tapauksessa tietoturva ei kykene tunnistamaan tapahtumaa hyökkäykseksi, vaan se tulkitaan tavanomaiseksi resurssien käytöksi. Sisäisiä uhkia aiheuttavat myös työntekijät, jotka vahingossa voivat tuoda haittaohjelmia järjestelmään. Tutkimuksien mukaan sisäpiiriläisten katsotaan olevan vastuussa 14 prosentissa kyberhyökkäyksistä. (Limnéll, 2014, 107)

Robert A. Grimes on määritellyt viisi yleisintä kyberuhkaa (Secureworks, 2017), jotka ovat:

1. Sosiaalinen manipulointi
2. Päivittämättömät sovellukset (kuten Java, Adobe Reader ja Flash)
3. Verkkourkinta eli kalastelu
4. Verkossa liikkuvat madot
5. Kehittyneet sitkeät uhat

Listan julkaisemisen jälkeen on kuitenkin alkanut levitä pelikenttää muuttavia teknologioita, kuten pilvipalvelut, Big Data ja mobiililaitteiden käytön omaksuminen. Yleisempiä kyberuhkien lähteitä ovat osavaltiot ja valtiot, terroristit, teollisuusvakoojat, järjestynyt rikollisuus, haktivistit ja hakkerit, kilpailijat liiketoiminnassa, tyytymättömät sisäpiiriläiset jne. Kyberuhat tyypillisesti muotoutuvat yhdestä tai useammasta seuraavanlaisesta uhasta:

- Aineettoman pääoman varkaudet
- Botnetit
- Datan manipulointi
- Datan tuhoaminen
- Informaation kalastelu
- Kehittyneet sitkeät uhat
- Mies välissä hyökkäykset (Man in the middle eli MITM)
- Malvertising
- Massamuistien ym. muistien tyhjennyshyökkäykset (Wiper attacks)
- Troijalaiset
- Palveluestohyökkäys eli DDoS (Distributed Denial of Service)
- Päivittämättömät ohjelmistot (Unpatched software)
- Rahavarkaudet
- Ransomware eli kiristysohjelma
- Vakoilu ja haittaohjelmat
- Valvomattomat ohjelmistot (Rogue software)

ENISA (European Network and Information Security Agency) käyttää uhkista koostuvaa kyberuhkien mallia. Uhkiin kuuluu erilaisia hyökkäyksiä ja teknologioita sekä haittaohjelmia, että fyysisiä uhkia. ENISAn mallin mukaan hyökkäysagentti on kuka tahansa henkilö tai asia, joka toimii (tai jolla on tarpeeksi vaikutusvaltaa) aiheuttaa, kantaa, levittää tai tukea uhkaa. Jotkut merkittävät uhka-agentit kyberavaruudessa ovat myös ENISAn mukaan yrityksiä, kyberrikollisia, työntekijöitä, valtioita ja terroristeja.

Yksi yleinen uhkamalli on viisiosainen luokitus, joka perustuu motivaatiotekijöihin, jotka ovat: kybervandalismi, kyberrikollisuus, kybervakoilu, kyberterrorismi ja kybersodankäynti. Edellä mainittujen uhkien motiivit voivat olla hyvin tyypillisesti itsekkyys, anarkia, raha, tuho ja valta. Myriam Dunn Cavelty on esittänyt rakenteisen mallin viisiosaisesta luokitusmallista (Lehto ym., 2015, 9):

Taso 1 Kybervandalismi. Se käsittää hakkeroinnin, haktivismin, internet-palveluiden eston ja internet-sivustojen saastuttamisen. Yksittäiselle yritykselle tai yksilölle kybervandalismi voi aiheuttaa merkittäviä taloudellisia menetyksiä. Viimeisimmät anonyymien hakkereiden aktiviteetit ovat olleet tehokkaampia kuin ne ovat aiemmin olleet.

Taso 2 Kyberrikollisuus. Euroopan yhteisöjen komissio määritteleekyberrikoksen seuraavasti: ”kyberrikollinen toimii digitaalisia kommunikaatioverkkoja ja informaatiojärjestelmiä hyödyntäen tai kyseisiä verkkoja tai järjestelmiä vastaan”.

Taso 3 Kybervakoilu. Tämä voidaan määritellä teoksi hankkia laittomin menetelmin salaista informaatiota (arkaluonteista, omistusoikeudellista tai yksityistä) yksilöiltä, kilpailijoilta, ryhmiltä, hallituksilta ja vihollisilta poliittisen, sotilaallisen tai taloudellisen hyödyn hankkimiseksi hyödyntämällä laittomia teknologioita internetissä, verkoissa, ohjelmissa tai tietokoneissa.

Taso 4 Kyberterrorismi. Se hyödyntää tietoverkkoja kriittiseen infrastruktuurin ja informaatioinfrastruktuuriin ja niiden valvonta- ja ohjausjärjestelmiin sekä internetpalveluihin kohdistuvissa hyökkäyksissä. Hyökkäysten tarkoituksena on aiheuttaa tuhoa ja pelkoa ympäristössä ja pakottaa poliittinen johto myöntymään terroristien vaatimuksiin.

Taso 5 Kybersodankäynti. Se koostuu kolmesta osa-alueesta, joita ovat strateginen kybersodankäynti, taktinen/operatiivinen kybersodankäynti ja kybersodankäynti matalan intensiteetin konflikteissa. Maailmanlaajuisesti ei ole olemassa yleistä kybersodankäynnin määritelmää, vaan sitä käytetään varsin vapaamuotoisesti kuvaamaan valtion toimintaa kyberavaruudessa. Lähtökohtaisesti kybersodankäynti vaatii sotatilan valtioiden välille, jossa kyberoperaatiot ovat osa sotilaallisia operaatioita.

Yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhat voivat samanaikaisesti tapahtua useassa yllämainitussa ulottuvuudessa. Esimerkiksi kyberoperaatiota ja toiminta, joka on tähdätty romahduttamaan vastustajan talouden, voi kuulua osaksi tavanomaista sodankäyntiä. Mitä tulee terrorismiin, erilaiset kybermaailman ja taloudellisen järjestelmän operaatiot voivat olla osana hyökkäyksiä, jotka aiheuttavat myös fyysistä tuhoa. Häiriöt voivat vaikuttaa ja lisääntyä ulottuvuuksien yli. Esimerkiksi luonnonkatastrofi voi aiheuttaa laajamittaisia häiriöitä sähköverkkoon, joka voi aiheuttaa haittoja maksujärjestelmiin ja ruoanjakeluketjuun. Pitkittyessään ne voivat aiheuttaa lisäksi siviileihin kohdistuvia haittoja (Lehto ym. 2015, 9)

2.3.2 Aktivismi kybermaailmassa

Vandalismia kybermaailmassa voidaan kutsua haktivismiksi ja se on poliittisesti, ideologisesti tai sosiaalisesti motivoitunutta toimintaa yhdistäen toimintana laittoman kansalaisaktivismin ja hakkeroinnin tekniikoita. Haktivismi muodostuu sanojen ”hakkerointi” ja ”aktivismi” yhteenliittymästä, vaikka sillä voidaankin viitata erilaisiin asioihin. Dorothy E. Denningin mukaan aktivismilla viitataan tavanomaiseen, häiriöitä aiheuttamattomaan kybermaailman hyödyntämiseen jonkin asian edistämiseksi. Tämä voi tarkoittaa esimerkiksi informaation hakua Internetistä, Web-sivujen ylläpitämistä tai luomista, digitaalisten julkaisujen ja informaation välittämistä ja toiminnan koordinoimista digitaalisin työvälinein. Aktivistinen toiminta, tai tässä tapauksessa Internetvahvisteinen aktivismi, on laillista toimintaa. (Limnéll, 2014, 114) ja Lehdon (2015, 10) mukaan kybervandalismi voidaan jakaa kahteen osaan, jotka ovat internet-vahvisteinen toiminta ja internetiin kohdistuva toiminta. Ensiksi mainitussa internetiä käytetään kommunikaatiokanavana tai tietoisuuden levittämistarkoituksessa. Viimeksi mainittu toiminta kohdistuu internettiin, sen palveluihin ja toimijoihin.

Haktivismi viittaa Denningin mukaan kybermaailmassa tapahtuviin operaatioihin, joissa hyödynnetään hakkeroinnin tekniikoita esimerkiksi kohteen Web-sivuille tunkeutumisessa. Toiminnan tavoitteena on häiritä tai keskeyttää sivun tai kohteen normaalit toiminnot, vaikkakin ilman vakavan vahingon aiheuttamista. Häirinnässä käytettyjä tekniikoita voivat olla muun muassa virtuaaliset istumalakot, sähköpostipommitukset, tietokoneisiin tunkeutumiset ja virukset sekä madot. Hyödynnettävät keinot voivat olla laittomia, laillisia tai jotain niiden väliltä. Haktivismi voi olla myös laittomien tai laillisuuden rajoilla olevien digitaalisten keinojen ja välineiden väkivallatonta käyttöä tiettyjen poliittisten päämäärien saavuttamiseksi. Toiminnassa korostuu väkivallattomuus, se voi olla laitonta tai laillista, lisäksi se hyödyntää kybermaailmaa ja se on poliittista. Globaalina tavoitteena voi olla vapaa ja rajoittamaton Internet sekä siihen liittyvä ilmaisun- ja sananvapauden edistäminen. (Limnéll, 2014, 114)

Nykyisin haktivismin vahvuutena voidaan pitää sen kykyä rekrytoida isot massat mukaan operaatioihinsa, johon muun muassa Anonymous tähtää. Haktivistiset ryhmittymät houkuttelevat uusia toimijoita mukaan jo pelkästään mahdollisuudella osallistua protesteihin ja tunnetun ryhmittymän nimissä. Ryhmän tunnettavuus takaa ja ylläpitää mediahuomiota, joka voi olla hyvin vetävä tekijä. Haktivistisista aktiviteeteista saadut tulokset ja aiheutuneet seuraukset voivat hyödyttää toisia kybertoimijoita. Tietomurron jälkeen esimerkiksi Internetissä leviävät salasana- tai henkilötietolistat voivat toimia niin hakkerin osaamisnäytteenä kuin palvella kyberrikollisuutta. (Limnéll, 2014, 118)

2.3.3 Kyberrikollisuus

Euroopan Yhteisöjen komissio määrittelee kyberrikollisuuden rikoksiksi, "jotka tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin". Tietoverkkorikollisuus voidaan komission mukaan jakaa kolmeen alaryhmään:

1. Perinteiset rikollisuuden muodot, jotka on tehty käyttäen hyväksi sähköisiä viestintäverkkoja ja tietojärjestelmiä. Tällaisia rikoksia voivat olla erilainen häirintä, uhkailu tai taloudellinen hyväksikäyttö.
2. Laittoman sisällön julkaiseminen sähköisissä viestimissä, kuten lapsen seksuaaliseen hyväksikäyttöön tai rasismiin liittyvän materiaalin levittäminen sähköisissä viestimissä.
3. Rikokset, joita esiintyy ainoastaan sähköisissä verkoissa, kuten hyökkäykset tietoverkkoa vastaan, palvelunesto tai hakkerointi.

Vielä muutamia vuosia sitten virusten kirjoittaminen oli nuorehkojen miesten harrastus, jolla he tavoittelivat huvia ja mainetta vertaistensa joukossa. Nykyisin verkkorikollisuus on ammattimaista toimintaa, jolla tavoitellaan taloudellista hyötyä. Rikolliset toimivat harvoin yksin, mutta eivät välttämättä muodosta kiinteää organisaatiota. Tyypillisintä on alihankinnan kaltainen yhteistyö, jossa rikolliset ovat omaksuneet eri rooleja. Taitava ohjelmoija voi kirjoittaa haittaohjelmia ja myydä niitä edelleen bot-verkon ylläpitäjälle. Ylläpitäjä puolestaan myy verkkonsa palveluja roskapostittajalle tai palvelunestohyökkäyksillä yrityksiä uhkaavalle kiristäjälle. Myös luottokortteja ja pankkitilejä kauppaavat tahot ovat taipuvaisia myymään tietonsa eteenpäin sen sijaan, että käyttäisivät niitä

itse. Nämä monimutkaiset ketjut tekevät rikosten selvittämisestä äärimmäisen vaikeaa, varsinkin kun syylliset voivat olla hajaantuneina eri puolille maailmaa. Monesti jäljet päättyvät maahan, jonka viranomaisilta puuttuu tahto, resurssit tai toimivalta tapausten selvittämiseen. Erityisesti Kiinan, Etelä-Amerikan osien sekä entisen Neuvostoliiton tiedetään houkuttelevan tai houkutelleen verkkorikollisia. Koska kiinnijäämisen riski on vähäinen, verkkorikollisuus on varsin kannattavaa toimintaa. Potentiaalisten uhrien joukko on niin laaja, että se korvaa pienen onnistumisprosentin tai vähäisen yksikköhyödyn. (Kääriäinen, 2010)

Nykyään kyberhyökkäyksissä käytettyjen virusten ja haittaohjelmien ohjelmointi on ammattimaista sekä taloudellista hyötyä etsivää aiemman harrastuksellisuuden ja maineen kalastelun sijasta. Taitava ohjelmoija voi ohjelmoida haittaohjelman (engl. malware) ja myydä sen esimerkiksi botnet-verkon operaattorille. Botnet-verkon operaattori taas voi edelleen myydä verkon palveluita roskapostittajille ja kyberavaruudessa toimiville kiristäjille, jotka uhkaavat yrityksiä palvelunestohyökkäyksillä. Monimutkaiset rikosketjut ja eri puolilla maailmaa toimivat kyberrikolliset tekevät rikosten ratkaisemisesta erittäin vaikeaa. Kyberrikollisuus on viime vuosina kasvanut huomattavasti ja aiheuttanut 40 % kasvua taloudellisissa seurauksissa. Yksittäisille organisaatioille ja pienyrityksille kustannusten nousu voi olla kohtalokasta. (Lehto ym., 2015, 3)

Rikosjäljet, kuten tekopaikka, tekotapa, rikoshyöty ja tekijä on mahdollista nopeasti tietotekniikan avulla häivyttää bittiavaruuteen. Rikosten ennaltaehkäisy-, torjunta- ja tutkintavastuu on useilla toimijoilla (Semecter, 2017). Semecter on jakanut ne seuraavasti:

- Vastuu verkkokäyttäytymisestä ja henkilökohtaisista suojausratkaisuista on jokaisella käyttäjällä itsellään.
- Vastuu ohjelmistohaavoittuvuuksien korjaamisesta on ohjelmistojen valmistajilla.
- Vastuu palvelun laillisuudesta, toimivuudesta ja turvallisuudesta on palveluntarjoajalla.
- Vastuu tietoteknisen infrastruktuurin toimivuudesta ja turvallisuudesta on operaattoreilla ja viranomaisilla.
- Vastuu tietoverkkorikosten tutkinnasta on poliisiviranomaisilla.

2.3.4 Kybervakoilu/tiedustelu

Tietojen hankinnassa kybermaailmassa ilmentyvät kybertiedustelu ja kybervakoilu. Näiden välille on vaikea tehdä tarkkarajaista määrittelyä, sillä se riippuu näkökulmasta. Toteuttajalle kysymys on laillisesta tiedustelusta, jonka kohde voi tulkita vakoiluksi.

Kybertiedustelu on julkisiin ja ei-julkisiin lähteisiin kohdistuvaa tiedonhankintaa, jonka tarkoituksena on kartoittaa ja lisätä ymmärrystä erilaisista uhista, riskeistä ja muutoksista niin maan sisällä kuin rajojen ulkopuolella. Tiedustelutoiminnan tavoitteena on tuottaa varhaisvaiheen tietoa, joka mahdollistaa uhkiin, riskeihin ja muutoksiin vaikuttamisen ja varautumisen. Tiedusteluun kuuluu tiedon analysointi, jonka avulla erilaisia turvallisuusympäristön epävarmuustekijöitä pyritään jäsentämään.

Kybervakoilua tulisi tarkastella laajennoksena traditionaaliselle vakoilulle. Sen avulla vihollinen voi varastaa tietoja etäyhteyttä hyödyntäen, halvalla ja teollisessa mittakaavassa. Kybervakoilua voivat vihollisen agentit toteuttaa suhteellisen pienellä riskillä. Britannian tiedustelupalvelu (MI5) pitää tämänkaltaista toimintaa tietokoneverkkojen hyväksikäyttönä. (MI5, 2018). Kybertiedustelua/vakoilua tapahtuu koko ajan ja eri maiden turvallisuusorganisaatiot pyrkivät hankkimaan sen avulla tietoa. Kybertiedustelu/vakoilutoiminnassa on mukana sekä valtiollisia turvallisuus/tiedusteluorganisaatiota että ulkoistettuja toimijoita, jotka enemmän tai vähemmän kiinteästi ovat yhteydessä tiedustelu/turvallisuuspalveluihin. Eri maiden asevoimat ovat muodostaneet omat kybersodankäyntiin liittyvät yksiköt, joilla on kyky kybertiedusteluun. (Lehto, 2015, 12)

Tiedustelun siirtyminen verkkoon on tapahtunut samassa tahdissa yhteiskuntien digitalisaation kanssa. Kybertiedustelun voimakkaan kasvun alku ajoittuu 2000-luvun puoliväliin. Kehittyneimmille vakoiluohjelmille on ollut tyypillistä, että ne on havaittu vasta vuosia operaation alkamisesta.

Vuonna 2011 havaittiin siihen saakka merkittävin verkkovakoiluoperaatio. Operaatiossa Shady RAT onnistuttiin tunkeutumaan 72 järjestön, yrityksen ja hallituksen järjestelmiin pääasiassa länsimaissa. Toiminta oli jatkunut jo viiden vuoden ajan.
Samana vuonna havaittiin verkossa Duqu-haittaohjelma, joka keräsi tietoa teollisuuslaitoksista kyberhyökkäysten valmistelemiseksi. Duqun arvioitiin toimeen verkossa neljä vuotta.

Vuonna 2012 löydettiin Flame-haittaohjelma, joka hyvin monipuolisesti kykeni käyttämään saastuttamansa tietokoneen resursseja. Se oli ensimmäinen usean megatavun kokoinen haittaohjelma, kun aikaisemmin ohjelmat ovat olleet kooltaan satoja kilotavuja. Haittaohjelmatartunnat keskittyivät Lähi-Itään. Tämän ohjelman arvioitiin toimineen verkossa viisi vuotta.

Vuonna 2013 raportoitiin NetTraveler-haittaohjelmasta, joka oli ollut toiminnassa vuodesta 2004. Tässä ainakin vuoteen 2016 jatkuneessa operaatiossa kohteena on ollut yli 350 organisaatiota 40 maasta. Hyökkäyskohteita ovat olleet avaruus-, nano, energia-, ydin-, laser- ja tietoliikenneteknologian sekä farmasian tietovarannot.

Vuonna 2014 havaittiin Regin-haittaohjelma, joka oli ollut käytössä jo vuodesta 2008 asti. Regin on enemmän ohjelmisto kuin yksittäinen ohjelma ja se oli tuolloin historian kehittynein ja monipuolisin. Tämä monitasoinen vakoiluohjelma kykeni hallitsemaan kohdettaan täydellisesti ja leviämään tehokkaasti. Kohteita oli ainakin 14 maassa.

Vuonna 2015 Yhdysvaltain Office of Personnel Management (OPM) ilmoitti, että se oli joutunut tietomurron kohteeksi, jossa siltä anastettiin noin 21,5 miljoonan liittovaltion työntekijän (nykyisiä ja entisiä) henkilörekisteritietoja kuten sosiaaliturvatunnus, nimi, syntymäaika ja -paikka sekä osoite.

Vuonna 2016 raportoitiin Remsec-haittaohjelma-alustasta (ProjectSauron). Sen arvioidaan toimineen vuodesta 2011. Kohteita sillä on ollut ainakin 30 useassa maassa ja se kykenee asentamaan takaovia, varastamaan tietoja ja tallentamaan näppäimistön käyttöä.

Keskeistä kehitykselle on ollut haittaohjelmien monimutkaisuuden ja kyvykkyyden kasvu samalla kun niiden havaitseminen on käynyt yhä vaikeammaksi.

2.3.5 Kyberterrorismi

Kyberterrorismi hyödyntää kyberhyökkäyksiä hyökättäessä kriittisen infrastruktuurin IT-järjestelmiä ja kontrollijärjestelmiä vastaan, tarkoituksenaan aiheuttaa haittaa ja levittää pelkoa ihmisten keskuudessa. Kyberterrorismi tähtää vaikutuksen aiheuttamiseen niin kansallisella kuin kansainväliselläkin tasolla. Kyberterrorismia on vaikea määritellä ja meneillään on keskusteluita, onko se erillinen ilmiö vai vain terroristien hyödyntämä informaatiosodankäynnin muoto. Kyberterrorismi mahdollistaa hyökkäyksien tekemisen ilman fyysistä riskiä. Sen keskipisteenä on aiheuttaa fyysistä vahinkoa IT-järjestelmille tai henkilöstölle sekä laitteistoille informaatioteknologiaa hyödyntäen. Kyberterroristeille tietoverkko on media, joka helpottaa kyberhyökkäyksien toteuttamista. Kybersodankäynnissä erilaisia kyberaseistuksia, kuten esimerkiksi haittaohjelmat, voidaan toimittaa kohteeseen tietoverkon välityksellä. Hyökkäyksen kohteina voi olla myös muita kuin tietoverkkoja ja hyökkäykset niitä kohtaan voivat merkittävästi heikentää hallitusten, asevoimien, sairaalajärjestelmien jne. toimintamahdollisuuksia. (Lehto, 2015, 13)

Kyberterrorismi voi hyödyntää muun muassa seuraavia toimintatapoja (Limnéll, 2014, 105 - 135):

- **Propagandan levittäminen**: Tiedon kokoaminen ja jakaminen, jolla vaikutetaan suureen joukkoon ihmisiä. Menettelemällä tällä tavoin voidaan tehostaa terroristiryhmien rekrytointia ja motivoida hakkereita tai muita osaavia ihmisiä osallistumaan terrorismiaktiviteetteihin.
- **Vandalismi:** Nettivandalismia ovat Internetissä olevien sivustojen tuhoaminen tai palvelunestohyökkäykset. Nettisivuille voidaan kirjoittaa väärää tietoa, joka voi tuhota sivun maineen tai olla muulla tavoin haitallista.
- **Palvelunestohyökkäykset**: Palvelunestohyökkäykset ovat toimintaa, jolla yritetään estää tietoresursseihin pääseminen tai niiden käyttö. Esimerkiksi yritysorganisaatiot voivat huomattavasti kärsiä informaation puutteesta ja sen vaikutuksesta päätöksentekoon.
- **Vakoiluohjelmat**: Tietoja varastavat vakoiluohjelmat voivat olla vaikeita havaittavia, jolloin hyökkäyksen kohde ei välttämättä ole niistä tietoinen.
- **Ohjelmien tai ohjelmistojen käskyjen muuttaminen**: Aiheuttaa ongelmia muun muassa kriittisen infrastruktuurin järjestelmissä tai sotilastietojärjestelmissä.
- **Kyberhyökkäykset siviili- tai sotilasinfrastruktuuria vastaan**: Kyberhyökkäyksiä toteuttava terroristi voi tunkeutua kriittisiin informaatioinfrastruktuureihin ja vaikuttaa tätä kautta koko yhteiskuntaan ja sen toimintaan.

- **Fyysiset hyökkäykset siviili- tai sotilasinfrastruktuurin keskeisiä laitteita kohtaan**: Laitteistoille voidaan aiheuttaa vahinkoja ja tai voidaan saattaa toimintakyvyttömiksi myös muilla tavoin kuin kyberhyökkäyksillä.

Ensisijaisesti kyberterrorismilla pyritään vaikuttamaan kriittisen infrastruktuurin toimintaan, josta suuri osa on haavoittuvaista, sillä se toimii keskitettyjen valvomo-ohjelmistojen (Supervisory Control and Data Acquisition eli SCADA) varassa. SCADA-ohjelmistoissa on graafinen käyttöliittymä automaatiojärjestelmiin, jonka avulla voidaan lukea liittymän kautta ohjelmoitavan järjestelmän muistia ja antaa sille uusia ohjeita. SCADA:n avulla voidaan siis ohjata ja valvoa automaatiojärjestelmien toimintaa. SCADA-ohjelmistoista erityisen haavoittuvaisia tekee se, ettei niitä ole alkujaan suunniteltu liitettäväksi Internetiin, eikä niiden kyberturvallisuutta ole siten kyetty varmistamaan. Lisäksi järjestelmät päivittyvät hitaasti ja niiden päivitysvälit voivat olla pitkiä. Todennäköisimpiä kyberterrorismin kohteita ovat kansallisen puolustuksen järjestelmät ja kriittisen infrastruktuurin toiminnan kannalta keskeisiä toimintoja tarjoavat järjestelmät. (Limnéll, 2014, 136)

2.3.6 Kybersodankäynti

Kybersodankäyntikäsitteelle ei ole yleisesti hyväksyttyä määritelmää ja sitä käytetään hyvinkin laajasti kuvaamaan erilaisia kyberympäristön tapahtumia ja toimia. Kybersodankäynnin käsite nousi voimakkaasti esille vuosina 2008–2010. Se syrjäytti osin aikaisemmin käytetyn informaatiosodankäynnin käsitteen, joka oli muotoiltu 1990-luvun puolivälissä. Toisille kybersodankäynti on sotaa digitaalisessa maailmassa, toisille se on vastakohta kineettiselle sodankäynnille. Tutkijoiden mukaan kybersodankäynnin määrittelyn tulisi perustua sodan tavoitteisiin ja motiiveihin, ei niinkään kyberoperaatioiden muotoihin. Sota on aina laaja-alainen kokonaisuus käsittäen kaikki sodankäynnin muodot. Kybersodankäynti on yksi sodankäynnin muoto, jota käytetään perinteisen kineettisen vaikuttamisen rinnalla. (Lehto ym., 2017, 194)

Kybermaailmassa verkkovakoilu ja palvelunestohyökkäykset ilman vakavaa fyysistä vahinkoa eivät ole kybersotaa. Perinteisessä sodankäynnissä esimerkiksi vieraan valtion rajojen sisäpuolelle tapahtuva luvaton tunkeutuminen sotilaallisin voimin voidaan katsoa olevan sotatoimi. Myöskin haktivistiryhmittymän aiheuttama massiivinen hyökkäys valtion kriittistä infrastruktuuria kohtaan on enemmänkin rikollista toimintaa kuin sotatoimi. Vakavat tietomurrot ja kybervakoilutapaukset ovat kuitenkin kehitystä kiihdyttäviä tapahtumia. Tämänkaltaiset tapahtumat voivat lopulta johtaa myös fyysiseen konfliktiin valtioiden välillä. Toisinaan sodan osapuolina voivat toimia myös ei-valtiolliset toimijat, mutta on tavanomaista, että ainakin yksi osapuoli on valtio. (Limnéll, 2014, 138 - 139)

Useat valtiot maailmalla ovat nostaneet kybermaailman sodankäynnin viidenneksi ulottuvuudeksi. Aiemmat neljä ulottuvuutta ovat olleet maa, meri, ilma ja avaruus. Yhdysvallat ja Venäjä ovat perustaneet kybersodankäyntiin erikoistuneita esikuntia ja joukkoja, jotka kykenevät kehittämään sotilaallista toimintakykyä ja doktriinia, eli oppijärjestelmää. Kybermaailma on tullut aiemman fyysisen maailman rinnalle luoden aivan uudenlaisen toimintaympäristön, joka auttaa sotilaallisessa vaikuttamisessa. Infrastruktuuria vastaan voidaan iskeä niin fyysisesti pommittamalla tai se voidaan myös toteuttaa joissain tapauksissa kyberhyökkäyksillä. Parhaimmillaan kyberoperaatiot voivat auttaa saavuttamaan tavoitteita, jotka olivat aiemmin mahdollisia vain käyttämällä fyysistä voimaa. (Limnéll, 2014, 140)

Kybersodankäynnissä kohteina ovat tavallisesti tietojärjestelmät ja/tai tieto, joka sisältyy näihin järjestelmiin. Kyberhyökkäyksen kustannukset ovat suhteellisesti halvempia kuin tavanomaisen sodankäynnin kustannukset. Luonteenomaista kybersodankäynnille on, että useimmiten kyberhyökkäyksessä on vaikeaa tunnistaa todellisia hyökkääjiä ja siten soveltaa voimankäyttövaltuuksia. Kyberhyökkäykset saattavat tuottaa väärän vaikutelman siitä, ettei kysymys ole vakavasta tapahtumasta, koska ihmishenkiä ei välttämättä menetetä. Hyökkäykset yhteiskunnan kriittistä infrastruktuuria vastaan saattavat kuitenkin aiheuttaa aineellisten tappioiden lisäksi myös ihmishenkien menetyksiä. Esimerkiksi laajamittaisella datamanipulaatiolla voi olla merkittäviä vaikutuksia yhteiskuntajärjestykseen kuin myös fyysisen voiman käyttöön vastatoimina. (Lehto ym., 2017, 194 - 196)

Kybersodankäynti nykyisessä muodossaan voidaan käsittää sisältävän informaatiosodankäynnin (Information Warfare, IW) ja elektronisen sodankäynnin (Electronic Warfare, EW). 2000-luvun alussa suomalaisen näkemyksen mukaan ”informaatiosodankäynti on yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista ja tältä suojautumista käyttämällä hyväksi informaatioympäristöä. Informaatiosodankäyntiä voidaan käydä yhteiskunnallisin, poliittisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin kaikilla sodankäynnin tasoilla. Informaatiosodankäynti koskee koko yhteiskuntaa ja on siten luonteeltaan pääosin turvallisuuspoliittista sekä toiminnallisesti valtakunnallista strategista tasoa koskettavaa toimintaa. Informaatiosodankäynnissä päämääränä on kansallisten tavoitteiden mukaisesti hankkia ja ylläpitää informaatioylivoima.”Elektronisen sodankäynnin keinoin hyökkääjä pyrkii vaikuttamaan informaation kulkuun siten, että johtamisen ja tulenkäyttöjärjestelmien luotettavuus alenee ja informaatiorakenteiden käytettävyys pienenee. (Lehto ym., 2017, 186 - 189)

Kybersodankäynnissä käytetään hyväksi globaaleja tietoverkkoja. 2000-luvulla erilaisista verkkohyökkäyksistä on tullut lähes jokapäiväistä toimintaa. Yhteiskuntaan kohdistuvan kyberuhan kohteista keskeisiä ovat kansallisen turvallisuuden kohteet sekä yhteiskunnan elintärkeät toiminnot, joilla turvataan kansalaisten elinmahdollisuudet. Keväällä 2007 Viroon kohdistui verkkohyökkäysten sarja, jonka kohteina olivat kolmen viikon ajan mm. valtiojohto, poliisi, pankkilaitos, media ja yritysmaailma. Päätoimintamuotoina olivat palvelunestohyökkäykset, joiden kohteina olivat mm. web-, e-mail- ja DNS-serverit

sekä reitittimet. Virolaisten mukaan tätä hyökkäystä ei voida pitää varsinaisena kybersodankäyntinä vaan se oli kyberkonflikti. Muodoiltaan siinä oli elementtejä, jotka antavat viitteitä valtiollisesta kybersodankäynnistä, mutta Viron oman määrittelyn mukaisesti kysymys oli sotaa alemmasta kyberkonfliktista, koska Viro ja Venäjä eivät olleet sotatilassa keskenään. (Ottis, 2008, 163 - 167)

Venäjän ja Georgian välinen sota, toiselta nimeltään Etelä-Ossetian sota oli elokuun 2008 ensimmäisellä viikolla Georgian sotavoimien ja Etelä-Ossetian armeijan sekä Venäjän federaation joukkojen välillä käyty sota. Useat georgialaiset ja eteläossetialaiset verkkosivut joutuivat jo 8. elokuuta palvelunestohyökkäysten kohteiksi. Georgialaisia sivustoja vastaan hyökkäys alkoi 9. elokuuta vastaisena yönä. Hyökkäykset kohdistuivat Georgian valtion ja presidentin sivustoille sekä Georgia-online-sivustolle. Georgian viranomaiset päättivät 11. elokuuta taistella ”disinformaatiota” vastaan ja keskeyttivät kaikkien venäläisten televisiokanavien lähetykset maassa. Georgian johtava internetyhteyden tarjoaja Caucasus Online esti pääsyn kaikki .ru-päätteen verkkosivulle. Venäjän uutistoimiston RIA Novostin sivuille hyökättiin ja ne kaatuivat muutamaksi tunniksi 10. elokuuta. Venäläisen englanninkielisen tv-kanavan RussiaTodayn sivuilla hyökättiin ja ne kaatuivat 12. elokuuta noin vuorokauden ajaksi. Georgian keskuspankin ja puolustusministeriön sivuille murtauduttiin, joissa kuvamateriaalia muutettiin.

2.3.7 Kyberoperaatiot

Kyberoperaatiot muodostavat kokonaisuuden, jolla horjutetaan vastustajan kybertoimintaympäristön tieto- ja informaatioperusteisia järjestelmiä sekä eri toimijoiden tilannetietoisuuden muodostumista. Samalla suojataan omia järjestelmiä sekä defensiivisin että offensiivisin keinoin. Kybersodankäynnissä kyberoperaatiot eivät ole kokonaan itsenäisiä, muusta sodankäynnistä erillään olevia operaatioita, vaan kiinteä osa kokonaisoperaatioita.

Kyberoperaatioissa korostuu vaatimus toiminnan nopeudesta ja laajuudesta. Puolustajan järjestelmät ovat alttiita kyberhyökkäyksille asevoimien koko taistelutilan laajuudessa. Kybersodankäynnissä ei ole rintamalinjoja vaan sodankäynti tapahtuu kaikkialla kybertilassa. Kyberhyökkäykset ja hyökkäysvektoreiden muutokset ovat hyvin nopeita. Sodankäynnissä on siirrytty päivä- ja tuntiluokasta minuutteihin ja sekunteihin. (Lehto ym., 2017, 199)

Useat valtiot kehittävät kykyään suorittaa operaatioita kyberavaruudessa maan, meren, ilman ja avaruuden lisäksi osana sotilaallista voimankäyttöä. Suorituskyky perustuu tiedusteluun ja vaikuttamiseen. Tiedustelulla pyritään selvittämään kohteen järjestelmien ja verkkojen kokoonpanoa ja haavoittuvuuksia sekä vastapuolen kykyä suorittaa kyberoperaatioita. Vaikuttamisen tavoitteena on saada aikaa haluttu poliittinen ja/tai sotilaallinen vaikutus vastapuolen järjestelmien ja verkkojen kautta. (Lehto ym., 2017, 199 - 200)

Kyberoperaatiot voidaan jakaa hyökkäyksellisiin toimiin (kybervaikuttaminen), puolustuksellisiin toimiin (kybersuojautuminen) ja tiedusteluun (kybertiedustelu) kybertoimintaympäristön eri rakenteissa. Kyberoperaatioita voidaan toteuttaa kolmella tasolla: strateginen, operatiivinen ja taktinen. Lisäksi kyberoperaatioita toteutetaan sotaa alemmissa konflikteissa osana sotilaallista, poliittista ja taloudellista painostusta. Kybersodassa kohteina voivat olla yhteiskunnan kriittinen infrastruktuuri, kansalaisten käyttämät palvelut sekä viranomaisten järjestelmät ja verkot. (Lehto ym., 2017, 200)

Kybersodankäynnin strategisen tason kyberoperaatioissa valtio pyrkii vaikuttamaan toisen valtion toimintaan sekä toimintakykyyn. Operatiivisella ja taktisella tasolla kyberoperaatioita suoritetaan osana muuta sotilaallista voimankäyttöä. Tavoitteena voi esimerkiksi olla sotilaallisen johtamisen häiritseminen, lamauttaminen tai harhauttaminen tai sotilaallisen voimankäytön estäminen tai viivästyttäminen. (Lehto ym., 2017, 200)

Kybersodan operatiivisella ja taktisella tasolla kysymys on kyberoperaatioista osana yhteisoperaatioita, joissa toimenpiteet kohdistuvat ensisijaisesti joukkojen johtamisjärjestelmiin. Näillä kyberoperaatioilla pyritään lamauttamaan vastustajan joukkojen tilannetietoisuuden muodostaminen sekä kyky tehokkaaseen joukkojen ja toiminnan johtamiseen. Sodan aikana toteutetuista kyberoperaatioista esimerkkinä voidaan pitää em. Venäjän ja Georgian välisessä sodassa vuonna 2008 esiintyneitä verkkohyökkäyksiä. (Lehto ym., 2017, 200)

Sotaa alempitasoisemman konfliktin yhteydessä valtiollinen toimija tai tämän tukema ja/tai suojaama ryhmittymä voi kohdistaa kyberhyökkäyksiä toista valtiota vastaan ilman, että valtiot ovat sodassa keskenään. Näille hyökkäyksille on tavanomaista, että tekijät pyrkivät pysymään tuntemattomina ja että valtiot kykenevät kiistämään osallisuutensa niihin. Näistä esimerkkinä on em. kyberoperaatiot Viroa vastaan vuonna 2007. (Lehto ym., 2017, 200)

2.3.8 Kyberaseistus

Kansainvälisesti tarkasteltuna kyberaseille ei ole globaalia määritelmää eikä riittävästi monialaista ja monitieteistä tutkimusta johtuen kyberaseistuksen profiilista, toiminnasta ja vaikutuksesta. Kyberaseistuksen määritteleminen on haastavampaa kuin perinteisemmän aseistuksen, kuten käsiaseet, räjähteet, joukkotuhoaseet, biologiset aseet, ydinaseet jne. Teknologian kehittyessä sodankäynti voidaan laajentaa ihmisen kehittämään alueeseen, kyberavaruuteen, jossa voidaan hyödyntää kyberaseita tukemaan tai voimistamaan konfliktia, joka pahimmillaan voi tehdä niistä todellisen uhan kansalliselle turvallisuudelle.

Kyberaseet voidaan nähdä kybersodankäynnin välineinä, jotka kykenevät lamaannuttamaan ja joissain tapauksissa tuhoamaan tietotekniikkaan perustuvia laitteita ja järjestelmiä. Kyberoperaatiolla voidaan myös epäsuorasti tuottaa ihmisille vammoja ja hengen menetyksiä. Vakoilutyökalujen tavoitteena on ollut kerätä dataa ja tiedustelutietoa, eikä niitä ole tarkoitettu tuottamaan fyysistä vahinkoa. Kyberaseen voi määritellä seuraavasti: tietokoneohjelma, joka on luotu ja/tai käytetty muuttamaan tai vahingoittamaan

järjestelmää, jotta sotilaalliset tavoitteet kyberavaruuden sisä- ja ulkopuolella olevaa vihollista vastaan voidaan saavuttaa. Tietokoneohjelma voi olla joko sovellus tai skripti, koska ohjelmointi- ja skriptikielet sallivat sekä datan että laitteistojen kontrolloinnin, jotka palvelevat erilaisia rooleja.

Kyberaseen tarkoitus on muuttaa, lamauttaa tai vahingoittaa väliaikaisesti tai pysyvästi kohdetta, kuten järjestelmää tai sovellusta, jotka voivat olla fyysisessä tai digitaalisessa maailmassa. Kyberaseen kohde voi olla myös sovellus, laite, data tai se voi olla järjestelmä, joka ei ole varsinainen IT-järjestelmä, mutta joka sisältää IT-komponentin ja sitä kautta IT-toiminnallisuuden. Kyberaseen vaikutus voi olla kyberavaruuden sisä- tai ulkopuolella ja sen vaikutus voi olla rajattu kohteena oleviin järjestelmiin tai sitä voidaan laajentaa muihin kohteisiin, kuten ihmisiin, vaikuttamalla ihmisten ja organisaatioiden käyttäytymiseen.

Kyberase voi olla luonteeltaan itsenäisesti liikkuva ja leviävä virus, mutta liikkuvuus ei ole välttämätön edellytys. Onnistuneimmat kyberaseet ovat luonteeltaan flegmaattisia, liikkuen varovasti vain lähiverkossa tai ei laisinkaan. Jälkimmäisessä tapauksessa kyberase on solutettava jokaiseen kohteeseen erikseen. Havaitut kyberaseet, kuten Stuxnet ja sen sukulaiset Flame, Duqu ja Gauss ovat modulaarisia hyökkäysohjelmistoja, joissa haluttu toiminnallisuus on koottu useammasta osasta. Näistä on selvästi tunnistettavissa varsinaisen toiminnallisuuden toteuttava taistelukärki ja sitä kuljettava lavettiosa. (Kiravuo ym. 2013)

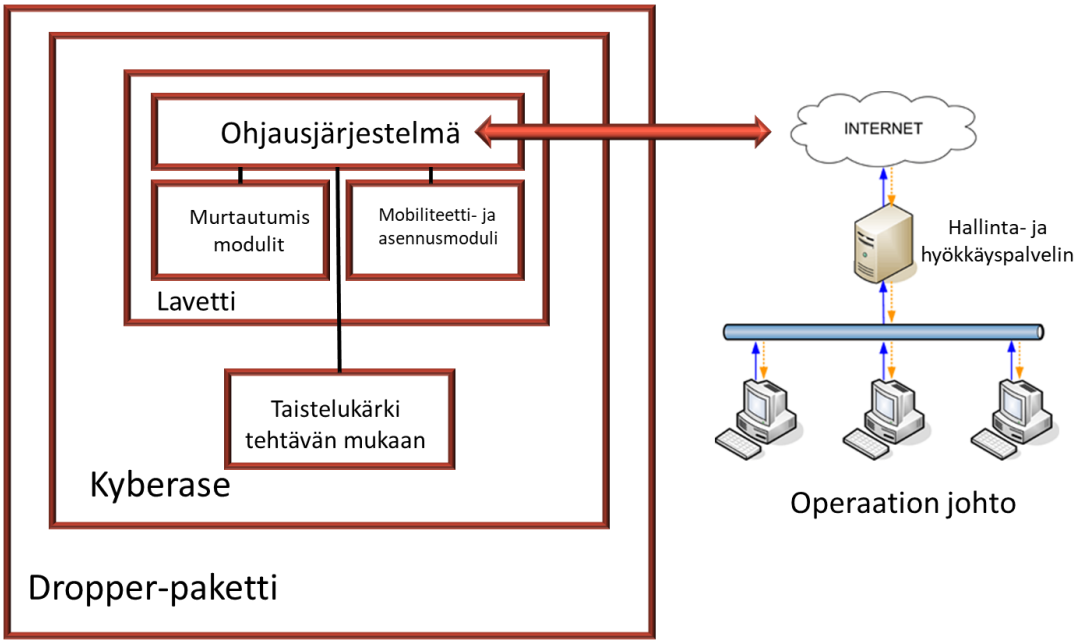
Lavettia ohjaa *ohjausjärjestelmä*, joka toimii täysin itsenäisesti tai pitää yhteyttä hallintapalvelimiin ja saa niiltä käskyjä. Ohjausjärjestelmä kohdistaa ja käynnistää taistelukärkikomponentit, se saattaa myös ladata uusia taistelukärkiä verkon kautta. Ohjausjärjestelmä hallitsee myös kyberaseen liikkuvuutta. (Kiravuo ym., 2013)

Jotta ase pääsisi kohteisiin, sen mukana on yksi tai useampia *murtautumismoduleita*, jotka on ohjelmoitu hyödyntämään tietojärjestelmien haavoittuvuuksia. Haavoittuvuuksia on erilaisia. Jokin saattaa esimerkiksi mahdollistaa oman ohjelmakoodin syöttämisen tietoliikenneohjelmalle siten, että se saadaan suorittamaan ohjelmakoodia. Toinen haavoittuvuus saattaa koostua tietyn automaatiojärjestelmän standardisalasanasta. Näiden haavoittuvuuksien kautta kyberase saa kohdejärjestelmän osittain haltuunsa ja saatuaan näin jalan ovenrakoon, pääsee se kopioimaan itsensä eteenpäin. (Kiravuo ym., 2013)

Varsinaisen kopioinnin ja liikkuvuuden toteuttaa murtautumismoduleita hyväkseen käyttävä *mobiliteetti- ja asennusmoduli*, joka asentaa aseen kohdekoneen käyttöjärjestelmään. Tunnetut kyberaseet osaavat hyödyntää käyttöjärjestelmävalmistajien sertifiointeja ja pystyvät siten asentumaan laiteohjaimina tai ohjelmistokirjastoina huomaamattomasti. Kyberase voi myös sisältää tässä kohdassa asentuvan rootkit-toiminnallisuuden, joka vaikuttaa käyttöjärjestelmään siten, että kyberaseen käynnissä olevia prosesseja ja tiedostojärjestelmässä olevia tiedostoja ei näytetä, kun järjestelmää tutkitaan. (Kiravuo ym., 2013)

Jos kyberase on suunniteltu leviämään kohdeorganisaation lähiverkossa, on se ensin saatava palomuurien suojaamaan verkkoon. Tämä voidaan saavuttaa esim. saastuneiden USB-muistitikkujen avulla tai lähettämällä kyberase sähköpostilla kohteeseen kuten Duqu-ohjelmaa on levitetty. Tällöin kyberase paketoidaan *dropper*-paketiksi, joka näyttää esimerkiksi tekstinkäsittely dokumentilta. Näistä moduleista koottu lavetti kuljettaa sitten mukanaan varsinaisen taistelukärjen tai useita sellaisia. Taistelukärki saattaa suorittaa tiedustelutehtävää, etsien tietyntyyppisiä tiedostoja kohdekoneesta tai verkkoliikevyiltä, lukien salasanoja näppäimistöltä, kuunnellen huonetta mikrofonin kautta jne. Toinen taistelukärki saattaa tehdä tuhoa, etsien automaatiojärjestelmiä ja rikkoen niitä, sotkien tietokantoja ja tehden muuta vahinkoa. (Kiravuo ym., 2013)

Kuvassa 14 on esitetty kyberaseen periaatteellinen rakenne (Kiravuo et.al. 2013).

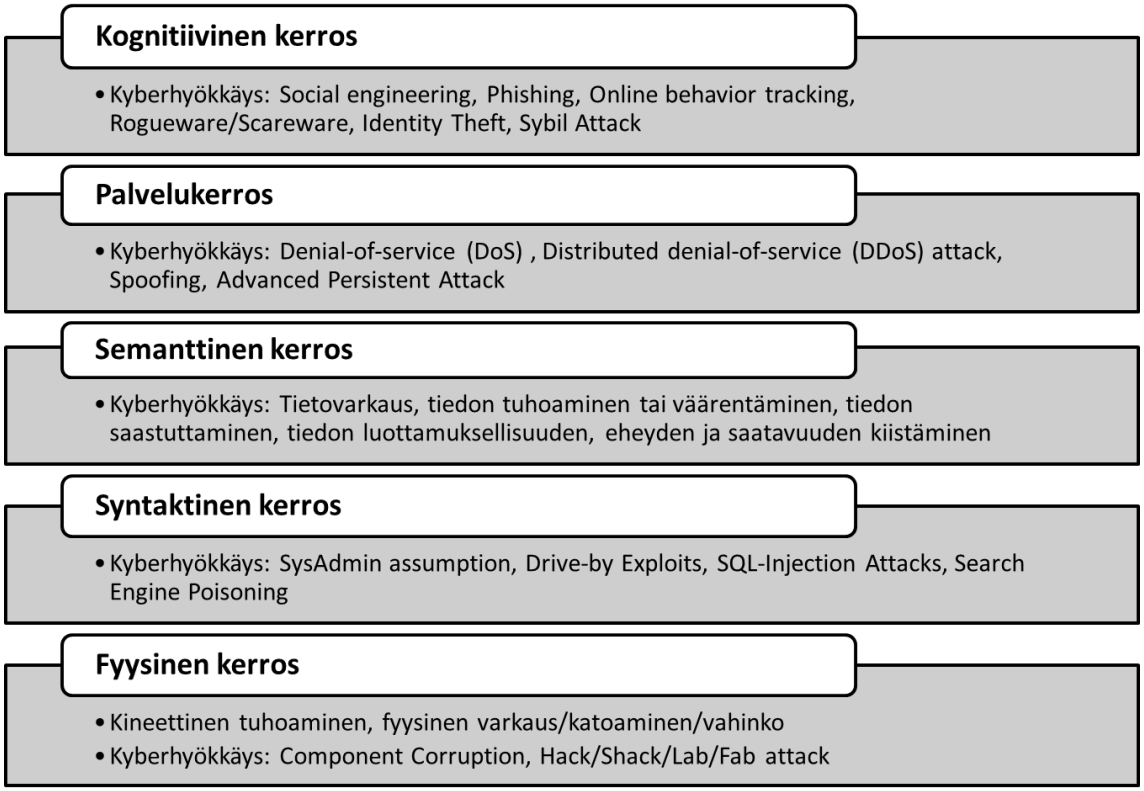


Kuva 14 Kyberaseen periaatteellinen rakenne (Bayuk, 2016, 20)

Kyberaseet koostuvat ryhmästä erittäin kehittyneitä tietokoneohjelmia, joiden toiminnallisuus määrittelee niiden kohteet. Kyberaseistusta käytetään kyberoperaatioissa, joiden tavoitteena on luoda haluttu vaikutus kohteessa haittaohjelmien avulla.

Eräs menestyneimmistä ja tunnetuimmista kehittyneistä kriittistä infrastruktuuria kohtaan kehitetyistä kyberaseista on todennäköisesti Stuxnet-mato, jonka kohteena oli Iranin ydinvoimaohjelma. Stuxnetin kohteena oli Siemensin toimittama sentrifugien ohjauslogiikka ja tehtävänä oli sabotoida laitteistoa ajamalla sentrifugien moottorit niiden toimintarajojen yli. Mato oli päässyt järjestelmään todennäköisesti saastuneen USB-tikun välityksellä. Stuxnetin ohjelmakoodi on tehty hyvin taitavasti. Se oli tiettävästi ensimmäinen mato, joka vakoilee ja uudelleenohjelmoi teollisuuden järjestelmiä.

ENISA käyttää uhkamalleja, jotka sisältävät teknologioita ja menetelmiä, haittaohjelmia ja fyysisiä uhkia. Hyökkäysmenetelmät ja tekniikat ovat mm: DOS- ja DDOS-hyökkäykset, hakukonehuijaukset, identiteettivarkaudet, informaatiovuodon väärinkäyttö, IP-osoitehuijaukset, kalastelu, kohdennetut hyökkäykset, luottamuksellisen tiedon vaarantaminen, näppäinpainallusten tallentaminen, roskapostitus, salasanojen murtaminen, sähköpostihuijaukset, jne. Yhdistämällä hyökkäysmenetelmiä ja -tekniikoita edellä kuvattuun kybermaailman tasomalliin, saadaan seuraavanlainen malli (kuva 15):



Kuva 15 Eri kybermaailman kerroksiin kohdistuvia hyökkäysvektoreita (Lehto, 2015, 21)

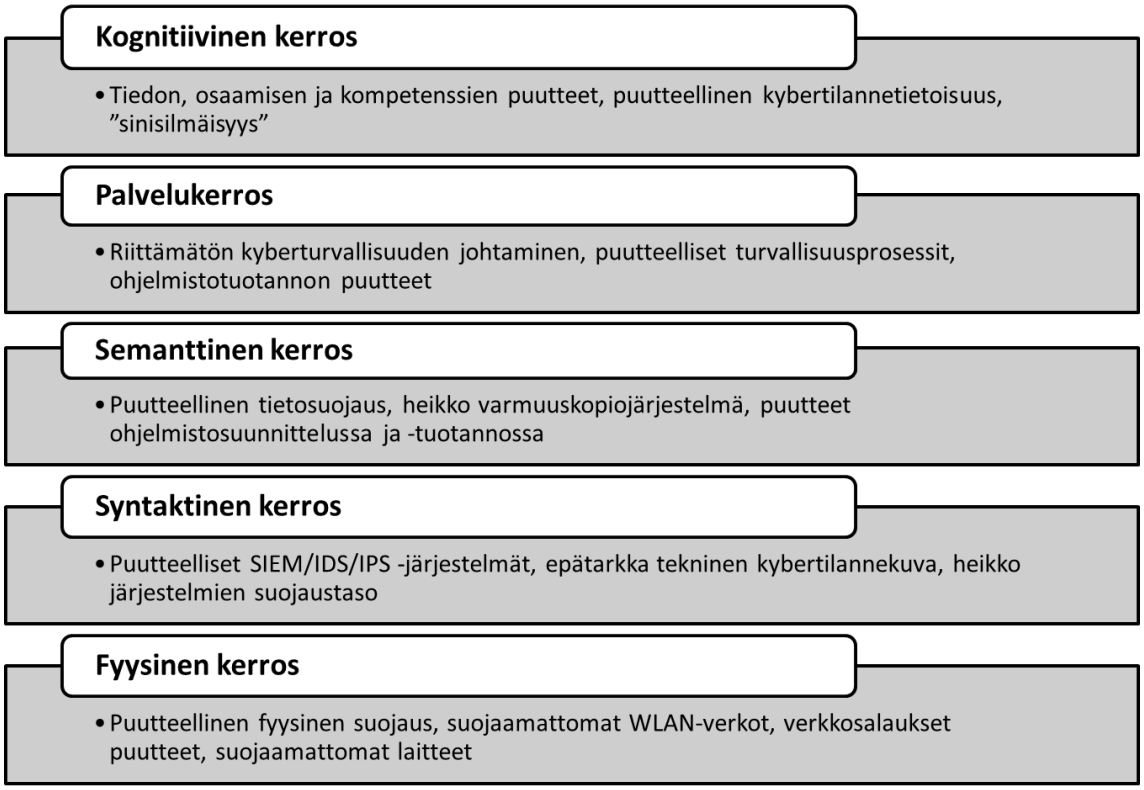
2.3.9 Kybermaailman haavoittuvuudet

Haavoittuvuudella tarkoitetaan informaatioteknologiassa vikaa tai heikkoutta, joiden avulla toimija kykenee heikentämään jonkin tietyn järjestelmän tieto- ja tai/toimintavarmuutta. Järjestelmässä voi olla vika tai heikkous, joita hyödyntäen hyökkääjä pääsee käsiksi järjestelmään ja siellä sijaitsevaan dataan, jota hän voi käyttää hyväkseen haluamallaan tavalla. Järjestelmän ylläpitäjä ja/tai omistaja kykenee haavoittuvuuksien systemaattisen tunnistamisen, luokittelemisen, korjaamisen ja lieventämisen avulla vähentämään niitä. (Limnéll, 2014, 110 - 111)

Haavoittuvuus voidaan ymmärtää uhkasta jäljelle jääväksi osuudeksi siten, että siitä on vähennetty kohteen sieto- ja palautumiskyky. Järjestelmän omistaja tai ylläpitäjä on sitä vähemmän haavoittuvainen, mitä parempi hänen sieto- ja palautumiskykynsä on. Kybermaailman ulkopuolella haavoittuvuudet ovat usein myös teknisiä ja ne voivat liittyä tietojärjestelmiin, tietoverkkoihin, kriittiseen infrastruktuuriin jne. Tärkeänä yhteiskunnallisena haavoittuvuutena voidaan pitää naiivia luottamusta yhteiskunnan tai sen ympärillä toimivan kybermaailman toimivuuteen sekä yhteiskunnan henkisen sietokyvyn puutetta. (Limnéll, 2014, 110 - 111)

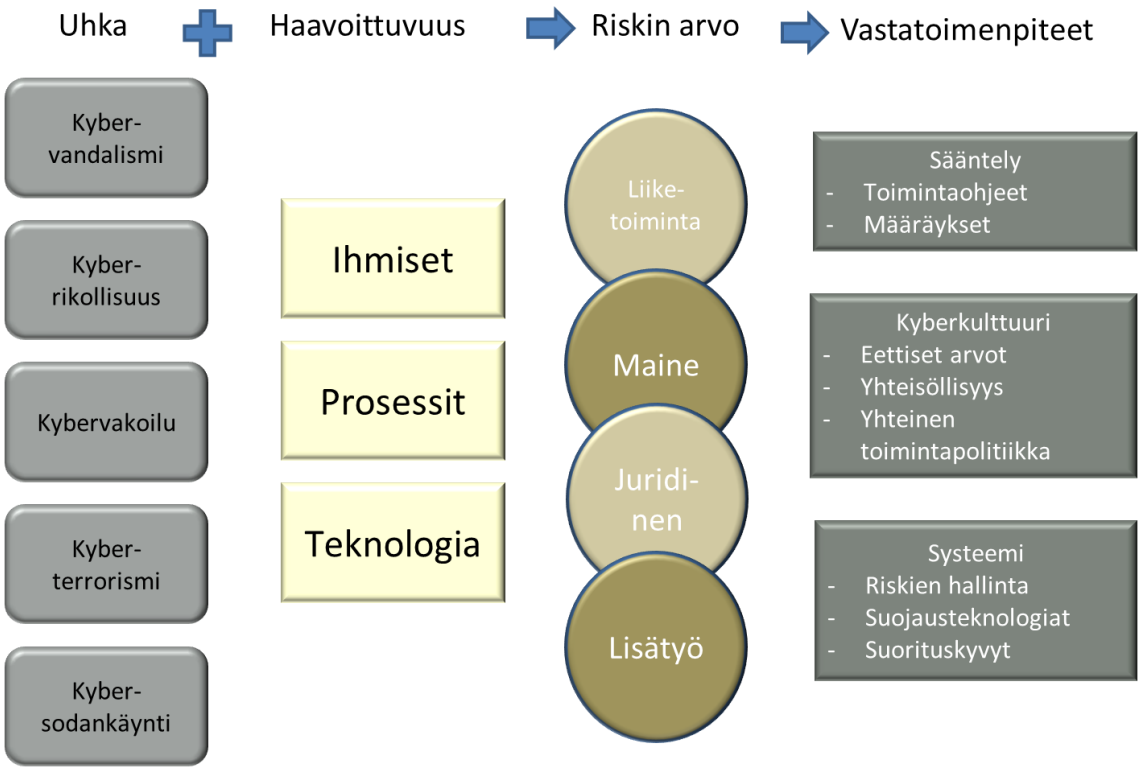
Viime aikoina haavoittuvuuksia on havaittu muun muassa sähköpostipalvelinohjelmistoissa, joita hyödyntämällä hyökkääjän voi olla mahdollista suorittaa omaa ohjelmakoodiaan kohdejärjestelmässä. Tämän kaltainen haavoittuvuus löytyi Exim-sähköpostiohjelmistosta, jonka ohjelmakoodissa oli virhe puskurin koon laskemisessa. Haavoittuvuuksia on löytynyt viime aikoina myös Samba-palvelinohjelmistoista, joissa haavoittuvuutta hyödyntämällä tunnistautuneen hyökkääjän on ollut mahdollista muuttaa kohdejärjestelmässä muiden käyttäjien salasanoja aina jopa pääkäyttäjän oikeuksilla oleviin salasanoihin saakka. Teoriassa hyökkääjä kykenisi suorittamaan mielivaltaisesti komentoja, laajentamaan käyttöoikeuksia, muokkaamaan tietoja, hankkimaan luottamuksellista tietoa ja ohittamaan suojauksia. (Kyberturvallisuus, 2018)

Kuva 16 ilmentää haavoittuvuuksia kybermaailman eri kerroksissa.



Kuva 16 Eri kybermaailman kerroksissa ilmeneviä haavoittuvuuksia (Lehto, 2015, 21)

Kyberturvallisuudessa uhka, haavoittuvuus ja riski muodostavat toisiinsa liittyvän kokonaisuuden. Lähtökohtana on jokin arvoa sisältävä fyysinen esine, tieto, osaaminen tai muu immateriaalinen oikeus, joka halutaan suojata ja turvata. Uhka (engl. threat) on jokin haitallinen kybermaailman tapahtuma, joka saattaa tapahtua. Uhan numeerinen arvo on todennäköisyys. Haavoittuvuus (engl. vulnerability) on järjestelmässä oleva heikkous, joka lisää tapahtuman todennäköisyyttä tai kasvattaa sen aiheuttamia vahinkoja. Haavoittuvuus voidaan jakaa ihmisten toiminnassa (engl. human factor), prosesseissa tai teknologiassa ilmentyviin. Riski (engl. risk) on vahingon odotusarvo. Se saadaan kertomalla todennäköisyys vahingon suuruudella. Riskiä voidaan tarkastella sekä taloudellisen arvon että maineen menettämisen kannalta. Vastatoimenpidekategorioita ovat: riskin poistaminen, riskin pienentäminen ja riskin hyväksyminen. Riskiä voidaan pienentää sääntelytoimenpiteillä, kehittämällä organisaation prosesseja ja yhteisöllisyyttä sekä kehittämällä teknologisia ratkaisuja. Kuvassa 17 on esitetty malli kyberuhkista, -haavoittuvuuksista, -riskeistä ja vastatoimenpiteistä.



Kuva 17 Kyberuhkien, -haavoittuvuuksien ja -riskien typologia (Lehto,2016)

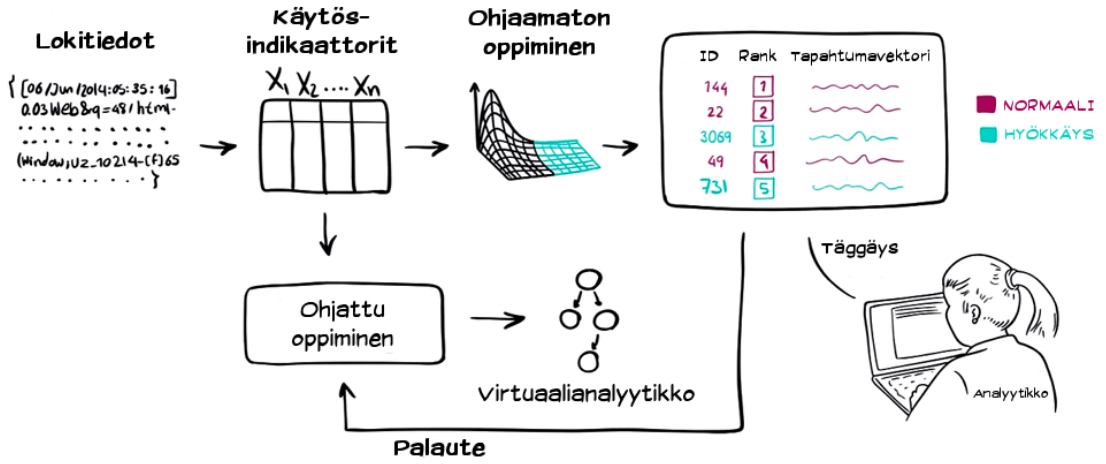
3 TEKOÄLYÄ HYÖDYNTÄVIÄ KYBERTURVALLISUUSRATKAISUJA

3.1 PatternEx AI2

Tekoäly ei vain sisällä uhka- ja riskitekijöitä vaan se voi toimia ongelmanratkaisijan asemassa. Tekoälyratkaisuja ja kognitiivista tietojenkäsittelyä sovelletaan kyberhyökkäysten havaitsemiseen, torjuntaan ja selvittämiseen.

Nykyaikaiset tietoturvaratkaisut useimmiten sijoittuvat jompaankumpaan seuraavista kategorioista: ihminen tai kone. Niin kutsutut analytiikkapohjaiset ratkaisut pohjautuvat sääntöihin, joita tietoturva-alan ihmisasiantuntijat ovat luoneet ja ne jättävät huomioimatta hyökkäykset, jotka eivät täsmää laadittujen sääntöjen kanssa. Koneoppimiseen perustuvat lähestymistavat luottavat anomalioiden tunnistamiseen, jotka voivat tunnistaa vääriä positiivisia tuloksia luoden sekä epäluottamusta järjestelmää kohtaan ja näin ollen vaativat ihmistyövoimaa tapauksia tutkimaan. (Dale, 1995)

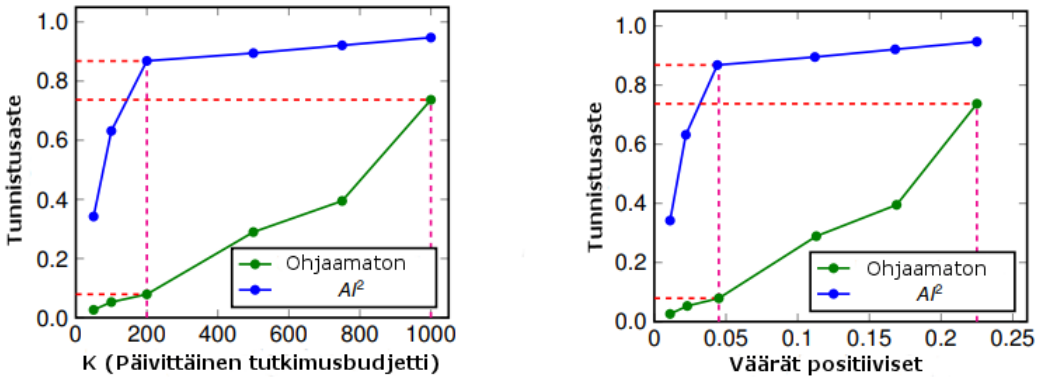
MIT:n Computer Science and Artificial Intelligence Laboratory(CSAIL) ja koneoppimiseen erikoistunut startup PatternEx kehittivät tekoälyalustan AI2, joka ennustaa tietoverkkohyökkäyksiä huomattavasti paremmin kuin nykyiset järjestelmät. Tutkimuksien mukaan AI2-alustan avulla kyettiin pääsemään 85 % hyökkäysten tunnistamistarkkuuteen, joka on noin kolme kertaa parempi tulos kuin aiempien tutkimuksien tulokset ovat olleet. Testit toteutettiin 3,6 miljardilla datakomponentilla (engl. log lines), joita generoivat miljoonat käyttäjät kolmen kuukauden tarkasteluajanjakson aikana. Hyökkäyksiä estääkseen, AI2 käy dataa lävitse ja tunnistaa epäilyttävän toiminnan klusteroimalla datan merkityksellisiksi malleiksi ohjaamatonta koneoppimista hyödyntäen (kuva 18). Tämän jälkeen lopputulokset esitetään analyytikoille, jotka varmistavat, mitkä tapahtumat ovat todellisia hyökkäyksiä. Analyytikot myös sisällyttävät lopputuloksen alustan malleihin (ohjattu oppiminen) seuraavaa analysoitavaa tietojoukkoa varten, jolloin järjestelmä oppii lisää. Järjestelmä kykenee myös jatkuvasti generoimaan uusia malleja jopa tunneissa, jolloin sen hyökkäysten tunnistamisten nopeus voi merkittävästi ja nopeasti parantua. (Conner-Simmons, 2016)



Kuva 18 Tekoälyohjatun AI2-alustan toimintaperiaate (Conner-Simmons, 2016)

Asiantuntijoiden aika on kuitenkin kallista, eikä heillä useimmiten ole aikaa käyttää järjestelmältä syötteenä tulevien epäilyttävältä vaikuttavaan toimintaan liittyvien ilmoitusten tarkastelemiseen. AI2:n yhtenä ominaisuutena on se, että siihen on sisällytetty kolme erilaista ohjaamattoman oppimisen metodia, jolloin järjestelmän tarvitsee lähettää asiantuntijoille arvioitavaksi vain tärkeimmät ja eniten huomiota vaativat tapahtumat. Tämän jälkeen järjestelmä kykenee rakentamaan ohjatun oppimisen mallin, jota se pystyy jatkuvasti parantamaan. Ensimmäisenä päivänä AI2 tyypillisesti valitsee 200 epänormaalia tapahtumaa asiantuntija-arviointia varten ja järjestelmän oppiessa ja tunnistusprosessin parantuessa tapahtumia voi tulla enää 30 - 40 päivittäin.

Kuvassa 19 havainnollistuu ohjaamattoman koneoppimisen ja AI2-alustan kustannukset toisiinsa verraten. AI2:n algoritmin avulla 86 % hyökkäysten tunnistusasteeseen voidaan päästä jo K:n ollessa 200, jolloin se on vielä alle 9 % koneoppimista hyödynnettäessä. K:n tulee olla hyvin suuri (yli 1000), jolloin käyrät voivat leikata eli budjetit ovat yhtä suuret. A2 toimii siis huomattavasti pienemmillä investoinneilla kuin ohjaamattoman koneoppimisen menetelmä yksinään. Kuvasta 45 voidaan myös havaita, että ohjaamatonta koneoppimista hyödyntäen voidaan saavuttaa 73,5 % hyökkäyksien tunnistusaste väärien hälytysten ollessa yli 22 % epäilyttävistä tapahtumista. AI2-järjestelmää hyödyntäen voitiin päästä 86 % tunnistustarkkuuteen väärien positiivisten ollessa 4.4 % luokkaa. (Veeramachaneni ym., 2016)



Kuva 19 AI2-alustan ja ohjaamattoman koneoppimisen vertailua (Veeramachaneni ym., 2016)

3.2 Amazon Macie

Amazon Macie on koneoppimista hyödyntävä tietoturvapalvelu. Tekoälyn avulla Macie kykenee löytämään, luokittelemaan ja suojelemaan sensitiivistä dataa Amazonin Web Palveluissa (AWS eli Amazon Web Services). Macie tunnistaa sensitiivisen datan, kuten henkilötiedot tai tekijänoikeudet. Lisäksi se kykenee monitoroimaan, miten tekijänoikeussuojattua materiaalia, kuten dokumentteja, kopioidaan, siirretään tai tarkastellaan. Maciessa on kojelautanäkymä, jonka avulla on pääteltävissä, miten dataa on käytetty ja minne sitä on siirretty. Palvelu jatkuvasti monitoroi datan käyttöä ja epäsäännöllisyyksiä sekä tuottaa yksityiskohtaisia hälytyksiä, mikäli dataan kohdistuu luvatonta käyttöä tai kyseessä on muutoin tahaton datavuoto. Macie kykenee myös automaattisesti tunnistamaan esimerkiksi liiketoiminnalliseen dataan kohdistuvan riskin, mikäli sitä on luvatta jaettu organisaation ulkopuolelle tai siihen on muulla tavoin tahattomasti päästy käsiksi. (Amazon Macie FAQ, 2018)

Amazon Macie käy lävitse dataa ja etsii siitä avainsanoja tiedostoformaateista, kuten Microsoft Word, Excel, txt-tiedostot jne. Macie vertaa tiedostoformaattien päätteitä arvioidessaan datan turvallisuustasoja. Esimerkiksi Macie sijoittaa .pem-loppuiset tiedostot korkeamman riskin luokkaan kuin .txt-tiedostot. Lisäksi Macie tarkastelee esimerkiksi tiedostoon ja S3 objekteihin liittyvää informaatiota turvallisuusluokitusta tehdessään. Macie hyödyntää myös Amazon CloudTrail-palvelua, joka kirjaa lokitiedostoihin lähes kaikki tehdyt API (Application Programming Interface)-rajapintakutsut sekä hyödyntää näitä lokitiedostoja tarkastellessaan objektitason S3-objektien API-aktiviteetteja. Lisäksi Macie kerää informaatiota käyttäjistä ja rooleista. (Stonefly, 2018)

Amazon Macien hyötyjä ovat muun muassa (Stonefly, 2018):

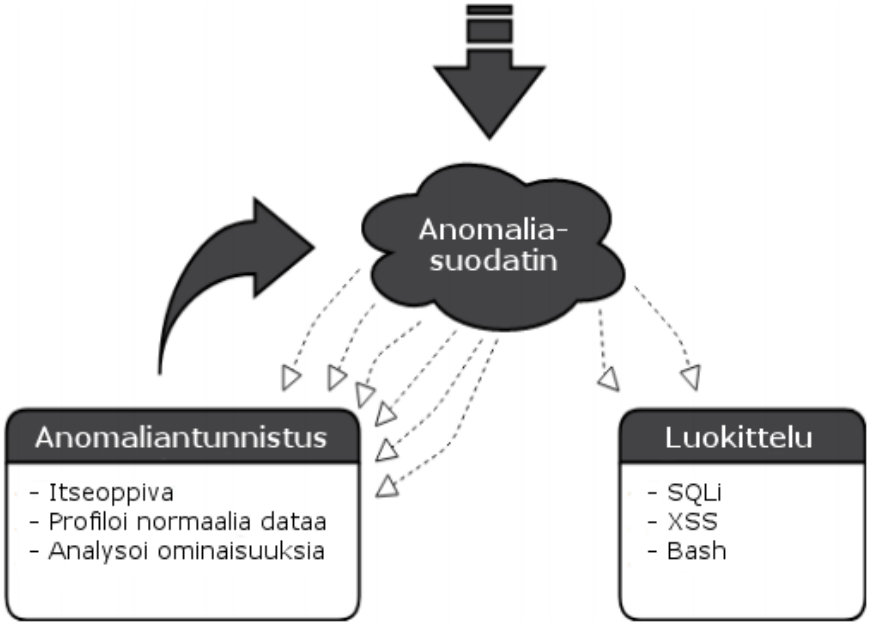
- Macie hyödyntää koneoppimista luokittelemaan Amazon S3-objekteja tarjoamaan datan näkyvyyttä S3-ympäristössä.
- Amazon käyttäjien käyttäytymisen analysointi (User Behavior Analysis) auttaa tunnistamaan epäilyttävää aktiviteettia.
- Amazon Macien avulla on mahdollista integroida tietoturvainformaatio ja tapahtumanhallintapalvelut työnkulun automatisoimiseksi.
- Macie tarjoaa 20 hälytyskategoriaa auttamaan varhaisten varoitusten generoimisessa.

3.3 Cyberlytic

Cyberlytic profiler on WWW-uhkien tunnistamiseen kehitetty työkalu, joka tunnistaa ja priorisoi hyökkäyksiä dataan kohdistuvien riskien suuruuden mukaan. Profiler analysoi kaikkea HTPP-protokollaan pohjautuvaa Web-liikennettä analysoimalla Web-palvelinpyyntöjä ja vastauksia sekä tuottamalla reaaliajassa kattavan riskiarvion, jota voidaan tarkastella kojelauta-käyttöliittymän (dashboard) kautta. Kojelauta-käyttöliittymä tarjoaa käyttäjille reaaliaikaisen yleiskuvan Web-uhkista. Raportit, kuten uhka-analyysi, hyökkäyksen kohteena olevat isäntäkoneet, riskin jakautuminen ajan mukaan ja hyökkäyksen aikajana, tarjoavat kuvan riskille altistumisesta. Profiler käyttää tekoälyä tunnistamaan kehittyneitä hyökkäyksiä, joita useimmat tavanomaiset WEB-sovelluspohjaiset sähköistä allekirjoitusteknologiaa hyödyntävät palomuuriratkaisut eivät kykene tunnistamaan. Profiler priorisoi työmäärän ilmoittamalla käyttäjälle, milloin korkean riskiluokituksen uhka on tunnistettu, jolloin ongelman korjaamisesta vastaavat IT-tiimit kykenevät puuttumaan asioihin. (Cyberlytic)

Profiler hyödyntää uudenlaisia strategioita poikkeavan käyttäytymisen analysoimiseksi Web-liikenteestä vähentääkseen sudenkuoppia, joihin tavanomaisiin allekirjoituksiin ja sääntöpohjaisiin teknikoihin perustuvat teknologiat ovat alttiita putoamaan. Nämä menetelmät auttavat reaaliajassa tunnistamaan yhä kasvavia ja kehittyneitä kyberuhkia vähentämällä ihmisen interventioiden tai interaktion tarvetta. Profiler käyttää Web-sovellusta ja ohjaamatonta koneoppimista analysoimaan datavirtoja. Itsenäisesti oppivat algoritmit profiloivat normaalia Web-liikennekäyttäytymistä tekemällä itse päätöksiä. Saavutetut mittarit ovat yksilöllisiä Web-palvelimelle ja ne sisältävät trendejä ja kausiluonteisia malleja. Kenttäominaisuudet sisältävät merkkijakson pituuden ja jakelun. (Cyberlytic)

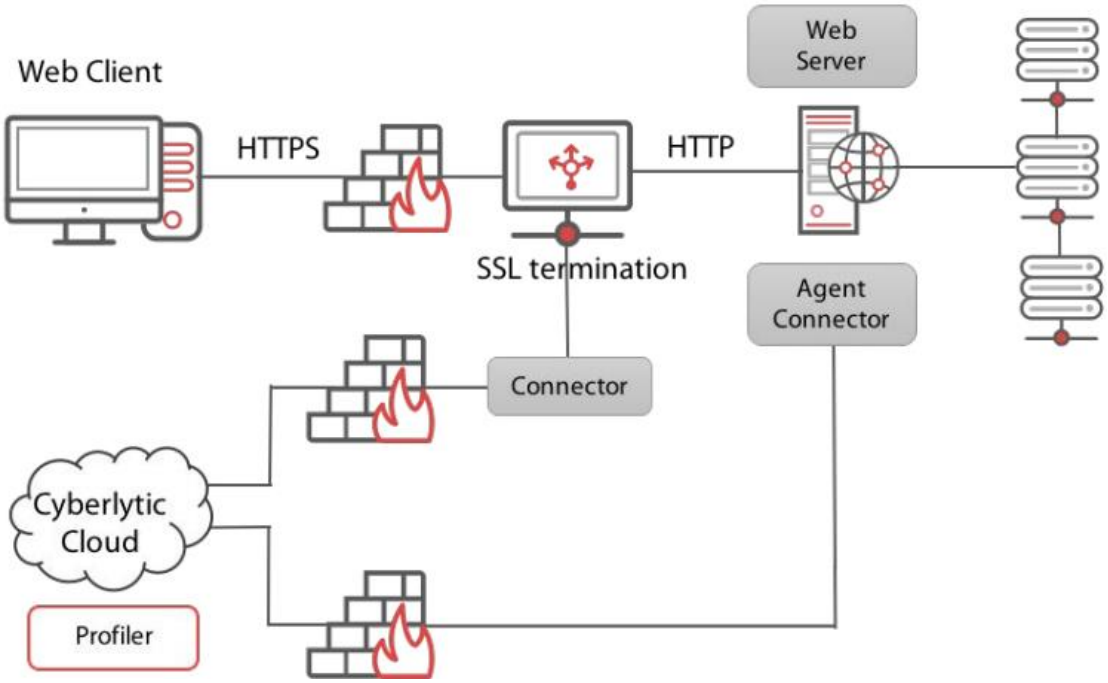
Web-sovelluksia profiloimalla Profiler kykenee määrittämään, ovatko lähetetyt pyynnöt peräisin tavanomaisesta tietyn Web-sovellusalueen sovelluksen jakelusta. Tämä lähestymistapa määrittää, miltä ”normaali” näyttää jollekin tietylle organisaatiolle. Sen seurauksena päätetään, mikä aikaansaa poikkeuksellista liikennettä alkuperäiseen lähtötilanteeseen verrattuna. Anomalioita tunnistamalla (kuva 20) voidaan korostaa erittäin todennäköistä häiriötoimintaa, jolloin ne voidaan riskiarvioida. (Cyberlytic)



Kuva 20 Cyberlyticsin ohjaamaton koneoppiminen web-uhkien torjunnassa (Cyberlytic)

Kaikki haitalliset anomaliat tuodaan esiin Profilerissa. Profiler käyttää patentoitua luokittelijalähestymistapaa määrittämään hyökkäyksen ominaisuuksia seuraaville hyökkäystyypeille: SQL Injection, Cross-site Scripting (XSS) ja Bash. Puolittain ohjattuja koneoppimisen algoritmeja käytetään määrittelemään Web-uhkien tyyppejä ja kolmea avainominaisuutta, jotka ovat: monimutkaisuus (engl. sophistication), valmiudet (engl. capability) ja tehokkuus (engl. effectiveness). Monimutkaisuus-ominaisuus määrittelee hyökkäyksessä käytetyn jonon laadun, valmiuksien avulla voidaan päätellä, onko hyökkääjä ihminen vai kone, ja tehokkuusominaisuus määritetään analysoimalla palvelimelta saatu vastaus, jotta voidaan nähdä, onko liikenne tavanomaista vai epänormaalia. (Cyberlytic)

Ominaisuuksia normalisoidaan koneoppimisen prosessin läpi, jotta voidaan määrittää jokaisen hyökkäyksen aiheuttama riski ja missä vaiheessa hyökkäyksen elinkaarta se on. Hyvin korkean tason riskiin voidaan arvioida esimerkiksi erittäin kehittynyt hyökkäys, jonka on toteuttanut taitava hyökkääjä ja jossa järjestelmä vastaa epänormaalilla tavalla. Profiler-ratkaisuun kuuluu kaksi ydinkomponenttia (kuva 21), jotka ovat Profiler ja Network Connector tai Agent. Käytössä ollessaan Profiler lähettää dataa tietoturvallisen verkkosyötteen yli Cyberlyticsin keskitetysti isännöimälle sovellusportaalille, joka sijaitsee Googlen Pilvipalvelussa. HTTP-raakadataa lähetetään Profilerille Web palvelimen Agent Connectorin ja Network Connectorin kautta. Web Server Agent Connector toimii tietynlaisena agenttina Web-palvelimelle ja se edelleenvälittää HTTP-istuntoja paikalliselle ja keskitetysti isännöidylle Profilerille analysointia varten. Network Connector toimii virtuaalisena laitteena, jolla on yhteys peilattuun kytkimen porttiin. Network Connector monitoroi kaikkea verkon liikennettä ja välittää vain HTTP-istunnot keskitetysti isännöidylle Profilerille, jotta ne voidaan analysoida. (Cyberlytic)



Kuva 21 Cyberlytic-pilvipalvelu ja Profilerin toimintaperiaate (Cyberlytic)

3.4 CylanceProtect

CylanceProtect on integroitu tietoturvauhkien estämiseen kehitetty työkalu, joka yhdistää tekoälyn tarjoamat hyödyt tietoturvakontrollien kanssa haittaohjelmainfektioiden estämiseksi. Tietoturvakontrolleja hyödynnetään suojautumisessa skriptipohjaisia, muistiin kohdistuvia ja ulkoisia laitteita hyödyntäviä hyökkäyksiä vastaan. Toisin kuin perinteiset tietoturvatyökalut, jotka perustuvat allekirjoitusten ja käyttäjien käyttäytymisen analysointiin ympäristössä esiintyvien tietoturvauhkien tunnistamisessa, CylanceProject:

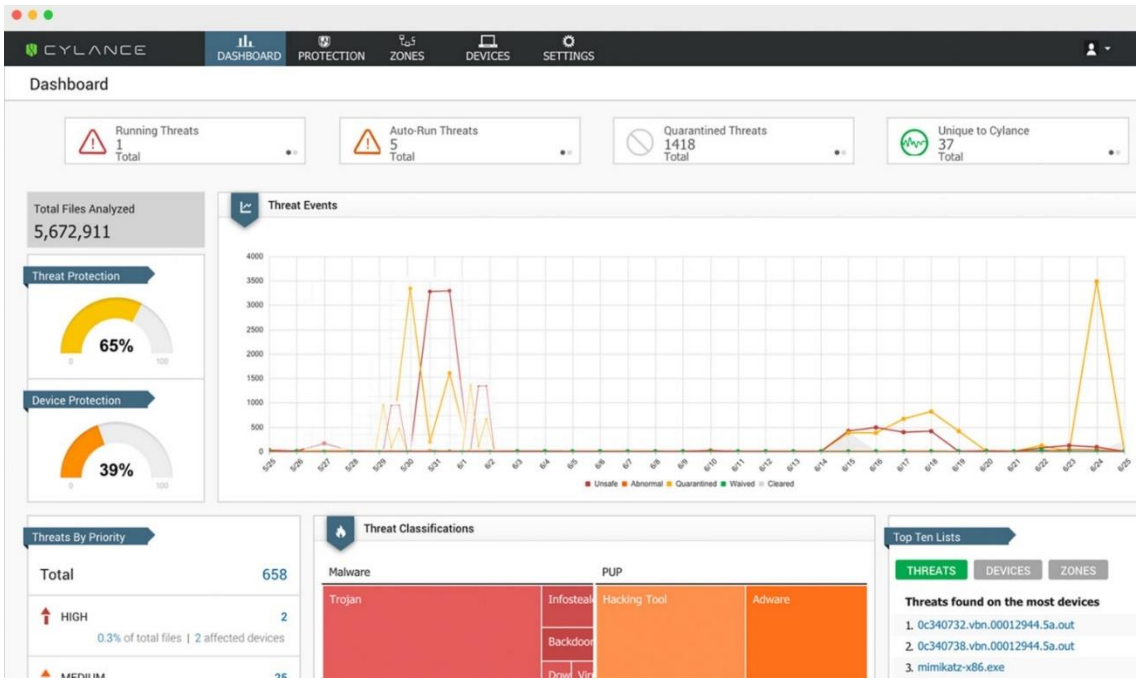
- Hyödyntää tekoälyä (ei allekirjoituksia) identifioidakseen ja estääkseen tunnettuja ja tuntemattomien haittaohjelmien suorituksen päätelaitteissa
- Ennaltaehkäisee tunnettuja ja tuntemattomia zero-day-hyökkäyksiä
- Suojelee päätelaitteita häiritsemättä loppukäyttäjää

CylanceProject-työkalun ominaisuuksia:

- Zero-day-hyökkäyksien estäminen on joustava tekoälymalli, joka estää zero-day-hyökkäysten toteutuksen.
- Tekoälypohjainen haittaohjelmien estäminen, jossa tekoäly tarkastaa kaikki sovellukset, joita ajetaan päätelaitteissa.
- Skriptien hallinta, joka kontrolloi milloin ja missä skriptitiedostot ajetaan sovellusympäristössä.
- Laitteen käyttöpolitiikan täytäntöönpano, joka kontrolloi, mitä laitteita voidaan käyttää ympäristössä eliminoimalla ulkopuoliset laitteet mahdollisena hyökkäysvektorina.

- Muistin hyväksikäytön tunnistaminen ja ehkäiseminen, joka tunnistaa proaktiivisesti haitallisen muistin käytön sekä toteuttaa välittömät automatisoidut ennaltaehkäisevät toimenpiteet.
- Sovellusten ohjaus kiinteätoiminteisille (engl. fixed-function) laitteille, mikä varmistaa, että kiinteätoiminteiset laitteet ovat ja pysyvät koskemattomassa tilassa.

Kuvassa 22 havainnollistuu CylanceProtect-työkalun kojelautanäkymä. Näkymästä voidaan saada informaatiota ajankohtaisista käynnissä olevista ja karanteenissa olevista uhkista, analysoitujen tiedostojen lukumääristä, prosentuaalisista suojaustasoista, uhkien luokitteluista ja prioriteeteista, eniten esiintyneistä uhkista jne.



Kuva 22 CylanceProtect-työkalun kojelautanäkymä (Cylance, 2018)

3.5 Darktrace

Darktrace on kyberturvallisuuteen keskittynyt matemaatikkojen perustama tekoälyä hyödyntävä yritys. Yritys soveltaa ihmisten immuunijärjestelmään liittyviä biologisia periaatteita vastatakseen haasteeseen suojella yrityksiä kehittyneiltä kyberuhilta. Darktracen teknologia auttaa yrityksiä reaaliajassa tunnistamaan tietoverkoissa tapahtuvia epänormaaleja tapahtumia jo ennen kuin ne kehittyvät haittaa aiheutuviksi kyberhyökkäyksiksi. (Darktrace, 2018)

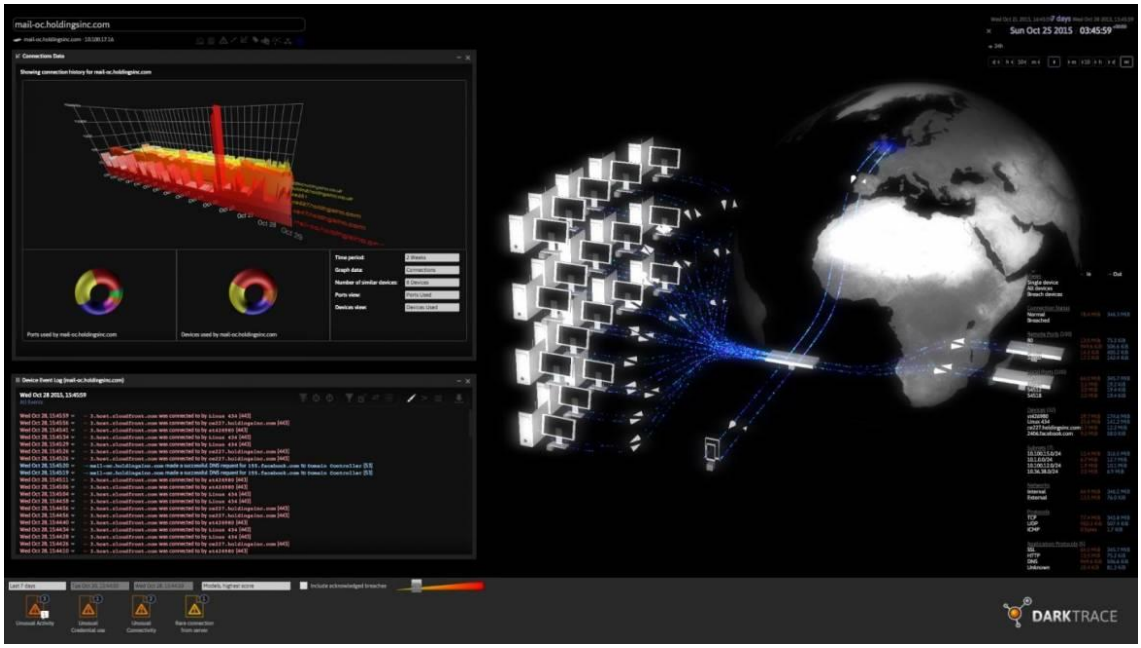
Darktracen tuote on tietoverkkoratkaisu, jonka avulla voidaan havaita ja tunnistaa kehittyviä kyberuhkia, jotka kykenevät kiertämään perinteiset tietoturvallisuusratkaisut. Darktrace käyttää Enterpise Immune System-teknologiaa (EIS), jonka toimintaa havainnollistetaan kuvassa 23. Se hyödyntää koneoppimista ja matematiikkaa, seuratakseen käyttäytymistä ja havaitakseen poikkeavuuksia organisaation tietoverkossa. EIS:n hyödyntäessä matemaattisia lähestymistapoja, se ei tarvitse allekirjoituksia tai sääntöjä,

vaan se kykenee tunnistamaan tuntemattomiakin hyökkäyksiä, jollaisia ei olla aiemmin nähty. EIS kykenee tunnistamaan ja vastaaman suurimpaan osaan taitavasti toteutettuihin verkossa piileviin kyberuhkiin mukaan lukien sisäpiiristä ilmenevät uhat. Koneoppimista ja matematiikkaa hyödyntäen EIS pystyy automaattisesti ja mukautuen oppimaan jokaisen käyttäjän, laitteen ja verkon tavan toimia tunnistaakseen käyttäytymismalleja, jotka ilmentävät todellisia kyberuhkia. Darktracen itseoppiva teknologia tarjoaa yrityksille kattavan näkyvyyden verkon toimintaan ja sallii niiden vastata ennakoivasti uhkiin ja vähentää riskiä. (Darktrace, 2018)

Kuva 23 Darktrace EIS-järjestelmän toimintaperiaate (Darktrace,2018)

Perinteinen tapa suojata informaatiota rakentamalla yhä korkeampia muureja ei ole riittävää nykyajan uhkien maailmassa. Cambridgen yliopiston asiantuntijoiden ottamat edistysaskeleet koneoppimisessa sekä matematiikan saralla mahdollistavat uuden aikakauden syntymisen kyberturvallisuudessa. Sen sijaan, että ennalta määriteltäisiin ”huonoja” käyttäytymismalleja ja luotetaan aikaisempiin hyökkäysmenetelmiin, Darktracen kehittynyt koneoppiminen yhdessä Bayesilaista todennäköisyysteorian kanssa osaa automaattisesti mallintaa ja yhdistellä tietoja sekä dynaamisesti että nopeasti. Darktrace monitoroi reaaliajassa verkossa siirrettyä raakadataa, kuten pilvipalveluidenkäytössä tapahtuvia interaktioita häiritsemättä esimerkiksi liiketoimintaoperaatioita ja transaktioita sekä tarjoaa välittömän näkymän kaikkeen digitaaliseen toimintaan ilmoittamalla käynnissä olevista hyökkäyksistä tai ilmenevistä poikkeavuuksista. (Darktrace, 2018)

Darktracen EIS-järjestelmän oleellisena osana on uhkien visualisointi (engl. threat visualizer), joka tarjoaa graafisen ja interaktiivisen käyttöliittymän. Sitä hyödyntäen analyytikot ja yritysjohtajat voivat visualisoida käyttäytymismalleja ja tutkia anomalioita, ilman tarvetta ymmärtää korkeampaa matematiikkaa, joka on järjestelmän taustalla. Uhkien visualisoija (kuva 24) tarjoaa käyttäjille reaaliaikaisen näkymän verkon informaatiovirtoihin ja suhteisiin. Poikkeamien ilmaantuessa visualisoijaa hyödyntäen käyttäjät voivat toistaa anomaliaan johtavia ja sen aikana tapahtuvia tapahtumia. Visualisoija on interaktiivinen työkalu, jolla analyytikot voivat tehdä yksityiskohtaisempia tutkimuksia ja suorittaa monimutkaisia kyselyitä. Visualisoija mahdollistaa myös syvällisen forensiikka-analyysin työkalulla, joka on käyttäjälle tai käyttäjän yritykselle soveltuva, kuten esimerkiksi Wireshark. (Darktrace, 2018)



Kuva 24 Darktrace visualisoijan graafinen käyttöliittymä (Darktrace, 2018)

Darktracen ytimessä on neljä matemaattista moottoria, jotka hyödyntävät useita matemaattisia lähestymistapoja, kuten rekursiivinen Bayesilainen estimointi. Ensimmäiset kolme mallia tuottavat käyttäytymismalleja yksittäisille ihmisille, laitteille joita he käyttävät, sekä yrityksille kokonaisuudessaan. Havaittaessa epätavallista käyttäytymistä yksi tai useampi näistä moottoreista lähettää viestin uhkien luokittelijalle (threat classifier), jonka tehtävänä on luokitella väärät positiiviset tapaukset ja raportoida aidoista poikkeamista, joiden tarkempi tarkastelu on mielekästä. Bayesilaisten lähestymistapojen kombinaatio, jota uhkien luokittelija korreloi ja mittaa, mahdollistaa tarkan poikkeamien tunnistamisen yrityksen mittakaavassa. Darktrace hyödyntää myös integroitua moduulia (model editor), jolla voidaan seurata ja valvoa toimintaperiaatteita. Tämä tukee muiden säännönmukaisuuskäytäntöjen- ja mallien määrittelyä, jotka voidaan räätälöidä asiakkaan erityisiin tunnistamisvaatimuksiin (esimerkiksi ei Dropbox-pääsyä, ei matkustusta arkaluonteisen informaatioteknologian kanssa tiettyihin maihin jne.) (Darktrace, 2018)

Terveydenhuollon teollisuudenala kohtaa yhä vaikeampia haasteita, kyberturvallisuuteen liittyen. Uudenaikaiset Internetiin kytkeytyvät laitteet, arkaluonteinen data ja usein tiukat tietoturvallisuusbudjetit vaikuttavat siihen, että terveydenhuollon alan yritykset sekä organisaatiot ovat säännöllisesti kyberhyökkäysten kohteena. Terveydenhuollossa Darktracen teknologia on osoittautunut hyödylliseksi alkuvaiheen kyberuhkien tunnistamisessa ja niihin vastaamisessa, mukaan lukien nopeasti muuttuvat kiristysohjelmat (ransomware) sekä aggressiiviset haittaohjelmat, jotka pyrkivät vaarantamaan pääsytietoja sekä haittaohjelmat, jotka pyrkivät purkamaan arkaluonteisia tietoja. (Darktrace, 2018)

3.6 Deep Instinct

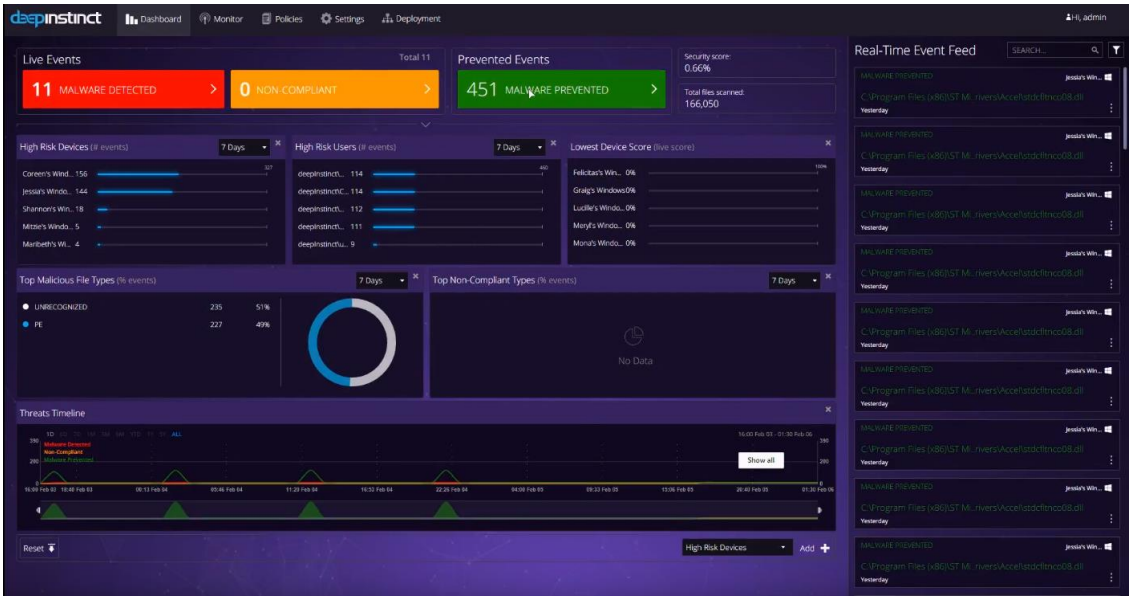
Deep Instinct on Israelissa vuonna 2014 Guy Caspin, Eli Davidin ja Nadav Maman perustama startup-yritys, joka on keskittynyt kehittyneen tekoälyn hyödyntämiseen kyberturvallisuudessa. Yrityksen päämajat sijaitsevat Israelissa ja San Fransiscossa. Deep Instinctin ohjelmisto (kuva 25) on suunniteltu suojelemaan organisaatiota, mobiililaitteita ja palvelimia tunnettuja ja tuntemattomia haittaohjelmahyökkäyksiä vastaan reaaliajassa. Yrityksen ohjelmisto perustuu keinotekoisten neuroverkkojen, jotka jäljittelevät ihmisaivoja, hyödyntämiseen. Kehittyneen tekoälyn avulla Deep Instinct kykenee tunnistamaan haitallisia ohjelmia mobiililaitteissa, palvelimissa ja työasemissa. Käyttämällä soveltuvia syväoppimisen algoritmeja ohjelmisto kykenee ennakoimaan ennalta tuntemattomia kyberhyökkäyksiä.

Deep Instinct on onnistunut hyödyntämänsä neuroverkkoteknologian avulla torjumaan hyökkäyksiä, kuten Spora, WannaCry, NotPetya ja Badrabbit ilman kyberturvallisuusasioihin keskittyvän keskuksen apua ja ennen kuin haittaohjelmilla on ollut minkäänlaista vaikutusta asiakkaiden IT-ratkaisuihin. Teknologia toimii rinnakkain perinteisien järjestelmien kanssa laajentamalla jo olemassa olevaa infrastruktuuria ja investointeja, jolloin asiakkaiden ei tarvitse tehdä korvaavia toimenpiteitä operaatioihinsa. Ratkaisut, kuten Deep Instinct, tähtäävät ennakoitavuuteen ja suurempaan toimintojen autonomisuuteen siten, että ihmisten tarvitsisi puuttua asioihin mahdollisimman vähän. Deep Instinctin etuna on myös se, että järjestelmä tarvitsee vain vähän päivityksiä ja se kykenee omaksumaan uudenlaisen ympäristön nopeasti vain vuorokauden ajanjaksolla tapahtuneen oppimisen jälkeen. (Arboleda, 2017)

Deep Instinctin kehittäjät hyödynsivät sovelluksen toteutuksessa syväoppimisen algoritmeja, joiden avulla oli mahdollista tunnistaa rakenteita, jotka viittaavat haittaohjelmiin. Deep Instinct kykenee tunnistamaan sekä estämään jo alkuvaiheen haittaohjelmien toimintaa kaikilla organisaation tasoilla. Toteuttaakseen syväoppimista, Deep Instinctin kehittäjät rakensivat suuren neuroverkon laboratorio-olosuhteissa ja opettivat sitä hyödyntämällä suurta määrää haittaohjelmista koostuvia näytteitä. Opetuksessa käytettiin tietokantoja, joihin oli kerätty kymmeniä miljoonia haitallisia ja harmittomia tiedostoja. Lopputuloksena saatiin ennustusmalli, joka voidaan lähettää suojattavalle laitteelle, jolloin voidaan käynnistää haittaohjelmien reaaliaikainen tunnistaminen ja estäminen. (Selden, 2016)

Ajatuksena on opettaa ohjelmisto tunnistamaan haittaohjelmiin viittaavia ohjelmakutsujen ja operaatioiden yhdistelmiä. Deep Instinctin oppimismetodi pilkkoo haittaohjelmanäytteitä hyvin moneksi pieneksi palaksi, jolloin haittaohjelma voidaan kartoittaa. Menetelmä on samankaltainen kuin genomisekvenssien selvitystapauksissa, sillä myös ne koostuvat useista kymmenistä tuhansista pienemmistä sekvensseistä. Nämä näytteistetyt palaset tuodaan neuroverkoille verkon opettamiseksi tunnistamista varten. Kyseinen neuroverkko suorittaa hyvin monimutkaista laskentaa, joten laskennan avuksi on toteutettu GPU-klusteri, jonka laskentakyvyt ovat huomattavasti CPU:n tarjoamia nopeampia. Lopputuloksena saadaan nopea ja vähän CPU-laskentatehoa vaativa staattinen neuroverkko, jota voidaan hyödyntää haittaohjelmien tunnistamisessa. (Selden, 2016)

Göttingenin yliopiston toteuttamassa haittaohjelmien tunnistustesteissä hyödynnettiin 16 000 haittaohjelmanäytettä, joita olivat keränneet Siemens CERT, Bit-Defender, McAfee, AVG, Kaspersky, Sophos jne. Edellä mainitut antivirusohjelmat kykenivät keskimäärin 61 % tunnistamistarkkuuteen, mutta Deep Instinctin keskiarvo oli 98,86 %. Jotkin haittaohjelmanäytteistä olivat jo automaattisesti mutatoituneita, mutta tavalla, joka ei vielä vaikuttanut kyseisten haittaohjelmien toimintaan. PDF-haittaohjelmilla tunnistusaste oli 99,7 % ja 99,2 % suoritettaville tiedostoille. Deep Insinctin sovellusta opetettiin 8000:lla näistä näytteistä koostetulla aineistolla. (Selden, 2016)



Kuva 25 Deep Instinct-sovelluksen graafinen käyttöliittymä (Google)

Perinteiset haittaohjelmien tunnistusohjelmat ovat yltäneet 80 % tunnistusasteeseen (kuva 26), joka jää lähes 20 prosenttia syväoppimisen algoritmeja hyödyntävistä sovelluksista (Tiquet, 2017; Google). Haittaohjelmien tunnistamista varten toteutetut sovellukset ovat kehittyneet jälkiin ja heurestiikkoihin perustuvien tunnistusmenetelmien ajasta sandbox-menetelmien (hiekkalaatikko, joka luo väliaikaisen rajoitetun alueen järjestelmän sisään ja jota voidaan käyttää mm. haittaohjelmilta suojautumiseen) kautta kone- ja syväoppimiseen perustuvia menetelmiä hyödyntäviin ohjelmiin. Deep Instinct edustaa siten uusinta teknologiaa haittaohjelmien tunnistamisessa.

Kuva 26 Haittaohjelmien tunnistusmenetelmien evoluutio (Google)

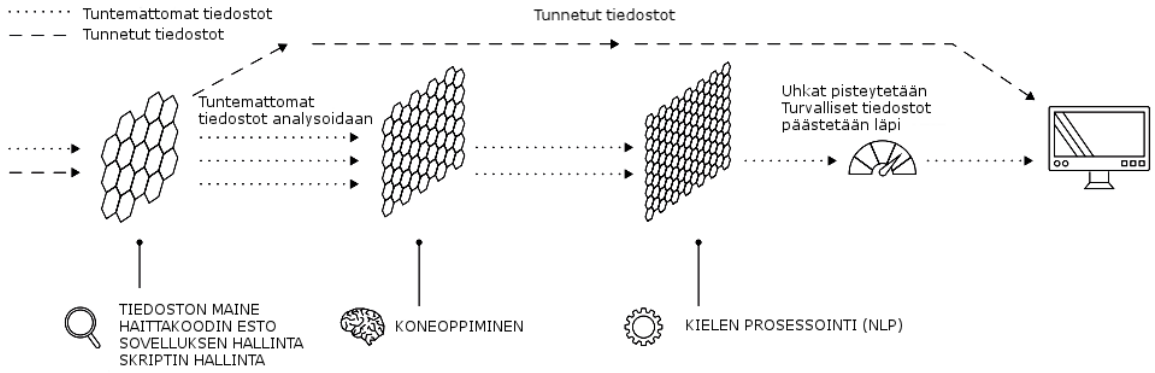
3.7 SparkCognition DeepArmor

Kyberrikollisuuden yhä kasvaessa ja muodostaessa yhä suuremman riskin maailmassa tapahtuvalle liiketoiminnalle, hallituksille ja kansalaisille on tarpeen kehittää työkaluja, joilla uhkaan voidaan puuttua. Rikoksien tekijöille kiinni jäämisen riski on matala ja rikoksen hyödyt voivat olla korkeat, mikä ei ole hyvä asia rikoksen uhrien kannalta. Tutkimusten mukaan kyberrikollisuus vaikutus globaaliin talouteen on jopa 600 miljardin Yhdysvaltain dollarin suuruinen. Nämä arviot ylittävät useiden maiden bruttokansantuotteen. Siitä huolimatta hallitukset ja yritykset eivät osaa ottaa uhkaa vakavasti, vaan aliarvioivat riskin ymmärtämättä, kuinka helposti jopa yksinkertaiset kyberhyökkäykset voivat häiritä heidän toimintojaan. (DeepArmor, 2018)

Asiaa monimutkaistavat sekä Internetiin yhteydessä olevien laitteiden eksponentiaalinen kasvu, että haittaohjelmat, jotka ylittävät yritysten tietoturvatiimien kapasiteetin. Organisaatiot joutuvat yhä enemmän panostamaan tietoturvaan informaatioteknologian, langattomien teknologioiden, IoT-laitteiden ja operationaalisen teknologian alueilla pysyäkseen ajan tasalla. Uudenlaiset uhkat vaativat kehittyneitä nykyaikaisia ratkaisuja yhä kehittyvällä kyberturvallisuuden sektorilla. Tähän saakka hyökkääjät ovat helposti voineet välttää allekirjoituksiin perustuvia virustorjuntaratkaisuja, mistä johtuen 95 % kybermurroista tapahtuu loppukäyttäjien päässä. SparkCognition DeepArmor kykenee tunnistamaan ja estämään haittaohjelmien, virusten, matojen, troijalaisten ja kiristysohjelmien uhkan hyödyntäen matemaattisia menetelmiä, kuten koneoppimisen metodeja ja luonnollisen kielen prosessointia. (DeepArmor, 2018)

DeepArmor-arkkitehtuuri koostuu pienestä päätelaitegentistä (endpoint agent), joka on integroitu pilvipohjaisen kognitiiviseen moottoriin ja uhkia tarkastelevan alustan kanssa. Päätelaiteagentti tunnistaa ja estää haittaohjelmia ja muita kehittyneempiä uhkia allekirjoituksista riippumatta. Agentti on suunniteltu suojelemaan asiakasta, palvelinta, mobiili- ja IoT-laitteita sekä tarjoamaan yhdistetyn tietoturvan koko yritykseen. Agentti voidaan myös konfiguroida toimimaan autonimisesti ilman käyttöliittymää tarjoten tietoturvaratkaisun IoT-laitteille. (DeepArmor, 2018)

Kuvasta 27 ilmenee, että DeepArmor-ratkaisun pilvipohjainen kognitiivinen moottori käyttää useampikerroksista suodatusprosessia uhkien tunnistamisessa. Ensimmäisessä suojauskerroksessa toteutetaan tiedostoanalyysi sekä sovelluksen- ja riskien kontrollointi, jolloin voidaan nopeasti tunnistaa tunnetut haitalliset ja poikkeavat tiedostot. Tunnistettujen tiedostojen suodattamisen jälkeen DeepArmor käyttää kognitiivisia algoritmeja, jotka tutkivat tuntemattomien tiedostojen DNA:n ja muodostavat uhkapisteytyksen jokaiselle tiedostolle. Uhkan tunnistamisen jälkeen pilvipohjainen hallintakonsoli (kuva 28) tarjoaa luonnollisen kielen prosessointityökalun (Natural Language Processing eli NLP). DeepNLP (kuva 29) ei vain etsi Internetistä evidenssiä uhkista, vaan myös ymmärtää uhkien ympärillä olevan kontekstin. Näin menettelemällä DeepArmor kykenee tarkasti erottamaan, mikä on todella haitallista pelkästään poikkeavista tapauksista. (DeepArmor, 2018)

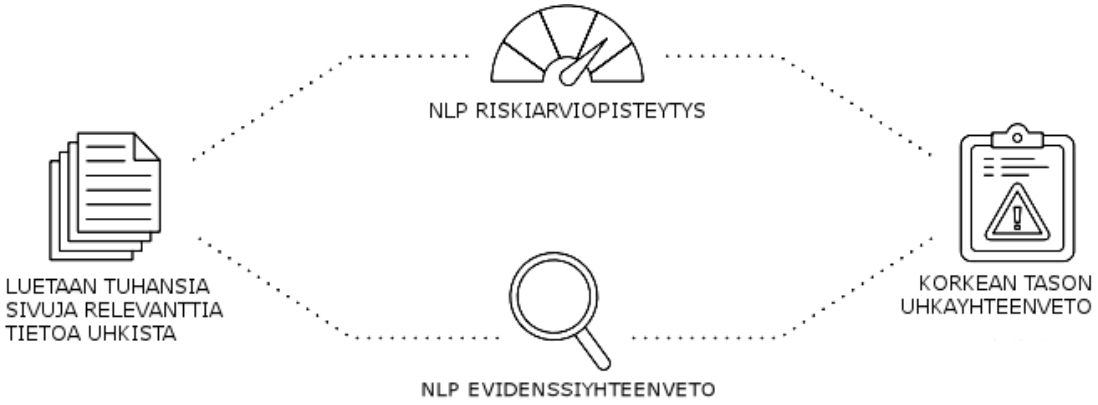


Kuva 27 Usean kerroksen lähestymistapa haittaohjelmien estämiseen (DeepArmor, 2018)

DeepArmor-hallintakonsoli voidaan asentaa osaksi SparkCongition pilviarkkitehtuuria tai se voidaan asentaa asiakkaan tiloihin Docker-säiliötä hyödyntäen. Joustava asennusarkkitehtuuri helpottaa ratkaisun käyttöönottoa ja hallintaa sekä mahdollistaa yritystason skaalautuvuuden. Hallintakonsolista voidaan nähdä laitteiden lukumäärät, tutkittujen tiedostojen määrät, uhkien aktiviteettiasteet, tunnetuimmat uhat, uhkatyypit sekä uhkien luokittelun ja osuuksien jaot prosenttiosuuksiin (mm. virukset, troijalaiset, madot, skriptit, botit, takaovet, kiristysohjelmat, rootkitit jne.) (DeepArmor, 2018)

Kuva 28 DeepArmor-hallintakonsoli (DeepArmor, 2018)

Kuvasta 28 havainnollistuu SparkCognition Deep NLP-teknologia eli luonnollisen kielen prosessointi. Teknologia toimii siten, että tietämyksen pohjaksi luetaan tuhansia sivuja relevanttia informaatiota uhkista, joiden perusteella voidaan ymmärtää uhkien ympärillä olevaa kontekstia. NLP-teknologia etsii myös Internetistä evidenssiä mahdollisista uhkista, joista tuotetaan evidenssiyhteenveto. Tunnetuista uhkista lasketaan lisäksi riskiarviopisteytykset, joita voidaan tarkastella hallintakonsolista. Lopuksi generoidusta informaatiosta voidaan tuottaa uhka-analyysiyhteenveto, jonka perusteella voidaan muodostaa toimintastrategiat ja puuttua ongelmiin, jotka ovat relevanteimpia. (DeepArmor, 2018)



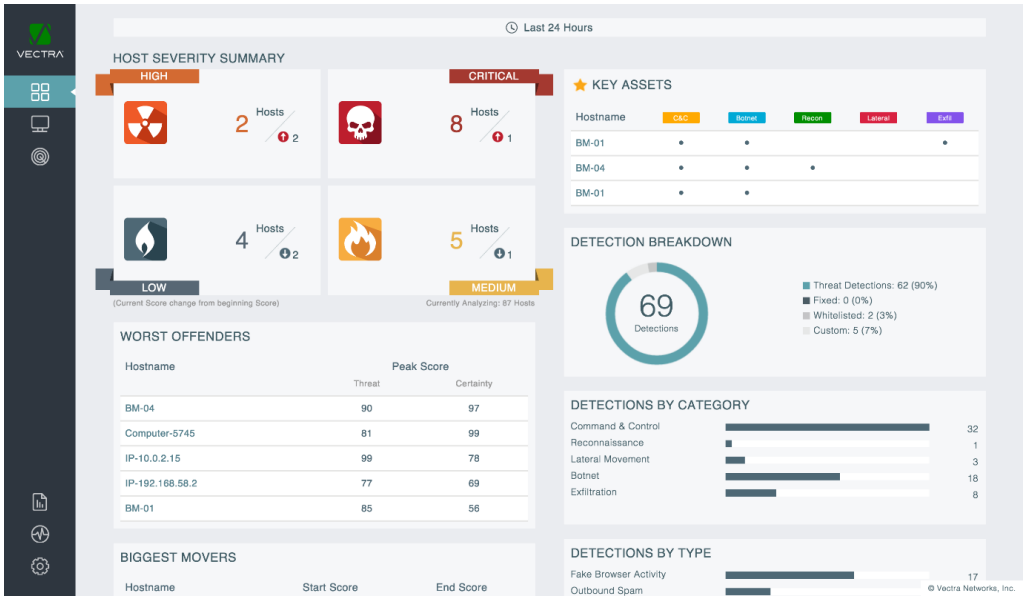
Kuva 29 SparkCognition Deep NLP-teknologia (DeepArmor, 2018)

3.8 Vectra Networks Cognito

Vectra Networks on vuonna 2010 perustettu ja vuonna 2012 rekisteröity Yhdysvaltalainen San Josessa, Californiassa, sijaitseva kyberturvallisuusuhkiin keskittynyt yritys, jonka tuotteet monitoroivat verkkoliikennettä identifioidakseen reaaliaikaisia Internetistä tai intranetistä kohdistuvia kyberhyökkäyksiä. Vectran tuotteita käyttävät yritykset toimivat toimialoilla, kuten rahoitus, terveydenhuolto, teknologia, sekä vähittäiskauppaan, että koulutukseen suuntautuneet yritykset. (Palmer, 2017)

Cognito on Vectran nopein ja tehokkain tapa löytää ja estää yrityksen verkkoon kohdistuvia kyberhyökkäyksiä. Se hyödyntää tekoälyä reaaliaikaisen kuvan muodostamiseen meneillään olevista tietoverkkohyökkäyksistä yksityiskohtineen, jotta niihin voidaan reagoida. Cognito yhdistää kehittyneitä koneoppimisen teknologioita, kuten syväoppimista ja neuroverkkoja jatkuvasti oppivien käsitemallien kanssa löytääkseen nopeasti ja tehokkaasti piilossa olevat ja tuntemattomat hyökkääjät, ennen kuin ne tekevät vahinkoa. Cognito eliminoi myös niin sanotut ”sokeat pisteet” analysoimalla kaikkea tietoturva- ja autentikointijärjestelmien sekä SaaS-sovellusten verkkoliikennettä ja lokitiedostoja. Tämä tarjoaa kattavan tilannekuvan käyttäjille ja IoT-laitteille pilvi- ja datakeskuksissa meneillään olevista prosesseista, jolloin hyökkääjille ei jää mahdollisuutta piilottautua. (Palmer, 2017)

Cogniton ”kojelauta”-käyttöliittymää (dashboard) on havainnollistettu kuvassa 30. Kojelauta priorisoi hyökkäyksen kohteena olevia työkuormia ja laitteita sekä vertaa niitä avainresursseihin ja tunnistaa koordinoituja hyökkäyksiä ja hyökkääjien aktiviteetteja. Kojelautanäkymästä havainnollistuu myös haittaohjelmien tunnistaminen kategorioittain sekä tyypeittäin ja tunnistettujen haittaohjelmien määrä. Kojelautanäkymä listaa myös pahimmat haittaohjelmat ja pisteyttää ne. (Palmer, 2017)



Kuva 30 Vectra Cogniton kojelauta-käyttöliittymä (Palmer, 2017)

Vectra Cognito hyödyntää kyberhyökkäysten torjunnassa ja tunnistamisessa kehittyneitä ohjattuja ja ohjaamattomia koneoppimisen tekniikoita, kuten syväoppimista ja neuroverkkoja. Perinteiset tietoturvajärjestelmät koettavat löytää hyökkäyksiä etsimällä järjestelmään kohdistuvista hyökkäyksistä tunnettuja allekirjoituksia (engl. signature) ja hyväksikäytön mahdollistavia aukkoja (engl. exploit). Cognito oppii koko verkossa tapahtuvasta toiminnasta pitkällä aikavälillä, kuten päivien, viikkojen tai kuukausien aikana. Cognito tunnistaa hyökkääjän verkkokäyttäytymisen kyberhyökkäysketjun jokaisessa vaiheessa. Tunnistettu hyökkääjän käyttäytyminen kategorisoidaan ja verrataan normaaliin palvelimien kanssa tapahtuvaan verkkokäyttäytymiseen, jotka on pisteytetty riskitasojen ja niiden määrittämisen suhteen. Hyökkäyskäyttäytymisestä tunnistetaan erityisesti sellaiset, jotka ovat osa yksittäistä koordinoitua hyökkäyskampanjaa. Tällöin ylläpitäjät voivat keskittyä suuntaamaan voimavaransa hyökkäyksiin, jotka aiheuttavat kaikkein suurimman liiketoiminnallisen riskin.

Yhteenveto tuloksista esitetään kaksiulotteisena uhkavarmuus-indeksinä, joka mittaa uhkatasoja. Palvelimet, jotka ovat merkittynä näkymässä keltaisella tai punaisella ilmentävät korkeaa tai kriittistä riskiä organisaatiolle, jolloin ne tulee käsitellä ensimmäisenä. Muut ilmentävät matalamman tason riskiä ja prioriteettia, jolloin niiden tilannetta voidaan arvioida myöhemmin. Palvelimia voidaan myös järjestellä sarakeotsikoittain. Cogniton tarjoama luokitteluominaisuus ja uhkien esittäminen tarjoavat ensimmäisen vaiheen luokitteluominaisuuden tietojärjestelmien ylläpitäjille. Hyödyntämällä tätä informaatiota, ylläpitäjät voivat nopeasti saada tilannekuvan tietyistä hyökkäyksen kohteina olevista palvelimista ilman, että heidän tarvitsisi tarkastella tuhansia erilaisia perinteisissä turvajärjestelmissä tapahtuvien tapahtumien aiheuttamia hälytyksiä.

Tiettyyn palvelimeen suuntautuvan hyökkääjän aiheuttaman hyökkäyksen käyttäytymismallin tunnistamisen jälkeen järjestelmän ylläpitäjät voivat tarkastella historiatietoja ja verkkoliikennettä, jotta he voivat määrittää hyökkäyksen todellisen syyn. Tällöin on mahdollista saada palvelin nopeasti karanteeniin ja tilanne korjattua. Historiatieto voi myös auttaa ylläpitäjiä saamaan käsityksen palvelimen infektoitumisen päivämäärästä, sijainnista ja luokittelemaan uusia infektoitumistiloja sekä rohkaisemaan järjestelmän käyttäjiä muuttamaan verkkokäyttäytymistään, jotta turvallisuustilanne voisi jatkossa parantua. (Palmer, 2017)

Cogniton käyttöliittymä ja työkalut lisäksi dynaamisesti visualisoivat hyökkääjän aktiviteetteja, jotka kohdistuvat verkon eri palvelimiin. Tällöin voidaan saada kokonaisvaltainen tilannekuva kaikista koordinoidun hyökkäyksen kohteena olevista palvelimista. Analyytikot voivat Cogniton avulla myös nähdä sekä palvelimet, jotka ovat tietyn hyökkäyskampanjan kohteena ja mitä toimenpiteitä on toteutettu palvelimien ja hyökkääjän välillä. Tämä mahdollistuu Cogniton alustan komentojen- ja ohjauksen tunnistuksella, joka tunnistaa kaikki palvelimet, jotka on yhdistetty samaan komento- ja ohjauskontrolli-infrastruktuuriin sekä korostaa asiaankuuluvia lateraalisia yhteyksiä palvelinten välillä. (Palmer, 2017)

3.9 Älykkäitä kyberturvallisuusratkaisuja

Tällä hetkellä useita kyberturvallisuusratkaisuja ja -työkaluja on tarjolla organisaatioiden tarpeisiin. Haasteena ovat ratkaisujen ja työkalujen fragmentaarisuus sekä uusien systeemien implementaation ja ylläpidon ongelmat, mitkä aiheuttavat koko järjestelmän kompleksisuuden kasvun ja hallinnan vaikeudet. Systeemien kompleksisuus edellyttää integroitujen järjestelmien kehittämistä, joissa on tunnistettu sekä ulkoiset että sisäiset uhat ja rakennettu kokonaisvaltainen kyberturvallisuusjärjestelmä.

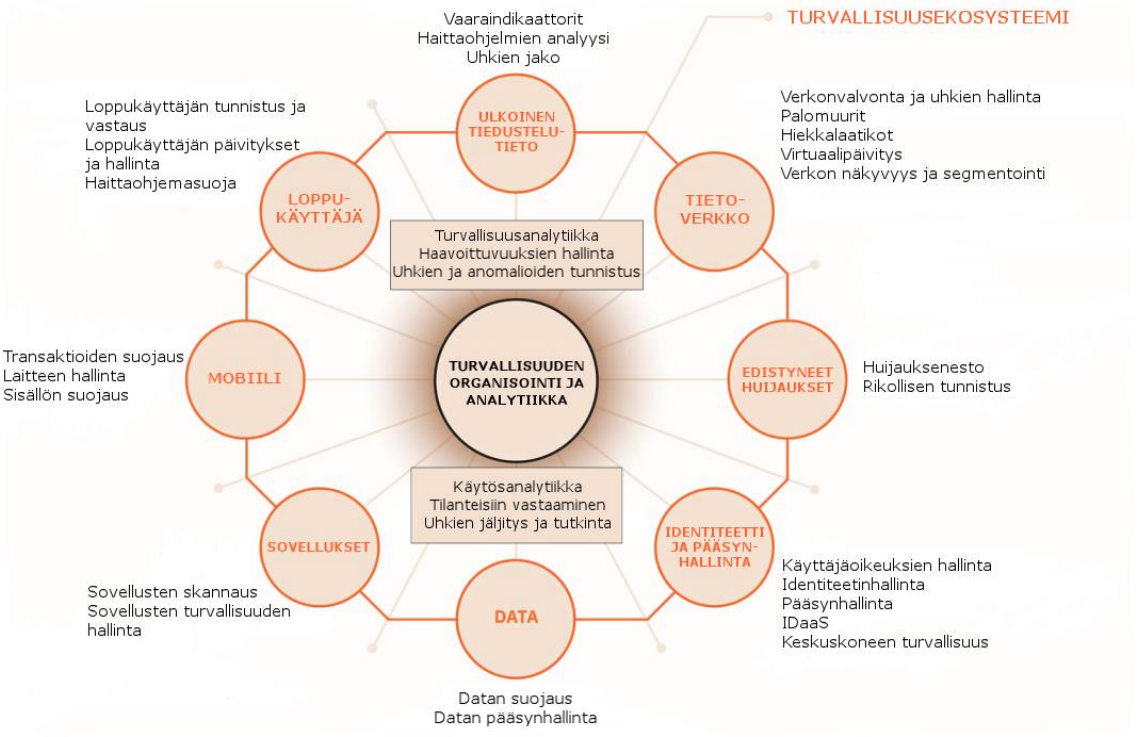
Järjestelmän tulee sisältää älykkäitä analyysiratkaisuja organisaation koko IT-infrastruktuurin alueella. Järjestelmällä tulee olla kyvykkyys nähdä sekä organisaation sisälle, että ulkopuoliseen maailmaan, joista uhat tulevat. IT-infrastruktuurin tulee sisältää itsessään tarvittavat turvallisuuskyvykkyydet. Järjestelmän tulee havaita oireet verkkohyökkäyksestä, kuten epänormaali kirjautuminen tärkeää tietoa sisältävälle palvelimelle tai epämääräisten pilvipalvelusovellusten käyttö ja reagoida siihen nopeasti. Uusia keinoja uhkien paljastamiseen tarvitaan, sillä organisaatio saattaa kohdata 200 000 tietoturvatapahtumaa päivässä. Tapahtumien tarkistaminen ihmistyönä on aivan liian hidasta ja kallista.

Integroiduilla ratkaisuilla saadaan tarvittava näkyvyys ICT-järjestelmän kaikille tasoille, jolloin suojautuminen ja torjunta voidaan toteuttaa kokonaisuutena eikä yksittäisinä toimenpiteinä. Tekoälyn kyvykkyys tulee esille erityisesti alkuvaiheen analyyseissä ja havaintojen läpikäynnissä. Tekoäly kykenee käsittelemään hetkessä satoja tuhansia asiakirjoja ja tietolähteitä. Tällä hetkellä julkaistaan päivittäin lähes 8 000 tietoturvaa käsittelevää artikkelia, joiden käsittelyyn ja hyödyntämiseen tarvitaan älykästä konetta.

Hyökkääjä käyttää hyväkseen organisaatioiden siiloutuneita ratkaisuja, joilla kuitenkin on vaikuttavuutta organisaation koko ICT-järjestelmään. Erityisesti perinteiset suojauskehiin perustuvat turvallisuusratkaisut eivät vastaa tämän päivän sofistikoituneisiin uhkiin organisaation ulko- ja sisäpuolella. Integroidussa turvallisuusjärjestelmässä luodaan vahva tietoverkon suojaus, päätelaitteiden hallinta ja turvallisuus, datavirtojen aktiivinen monitorointi, havaintokyvykkyyden luominen ja erilaisten hyökkäysvektoreiden torjunta. Järjestelmä edellyttää kyvykkyyttä ymmärtää alati muuttuvaa hyökkäysalaa ja uusia hyökkäysvektoreita. Älykkäästä kyberturvallisuudesta muodostuu alusta, joka tarjoaa laajan ekosysteemin integroituja turvallisuusratkaisuja. Alustaratkaisu mahdollistaa tehokkaan kyberturvallisuusasiantuntijan ja tekoälysovelluksen yhteistyön, jossa tekoäly toimii avustavan asiantuntijan roolissa toteuttamalla tarvittavia toimenpiteitä ja samalla tuottamalla jalostettua informaatiota päätöksenteon pohjaksi.

3.10 IBM Security-tietoturvaratkaisu

IBM:n tietoturvaratkaisu (IBM Security, 2018, kuvio 31) on integroitu ratkaisu, joka auttaa organisaatioita tunnistamaan, kohdistamaan ja estämään tietoturvauhkia. IBM security on konsepti integroidusta kyberturvallisuusratkaisusta, jossa analytiikkakyvykkyys on asetettu ratkaisun keskiöön. IBM:n tietoturvaratkaisuun kuuluvat ohjelmistot toimivat samankaltaisesti kuin immuunijärjestelmä estäen ja korjaten kyberhyökkäyksien aikaansaamia vahinkoja, joita on kohdistunut organisaation tietoturvaan. IBM Security koostuu kahdeksasta osasta, jotka ovat ulkoinen tiedustelutieto (threat inteligence), tietoverkko (engl. network), edistyneet huijaukset (engl. advanced fraud), identiteetti ja pääsynhallinta (engl. identity & access), data, sovellukset (engl. apps), mobiili (engl. mobile) ja loppukäyttäjä (engl. endpoint). Tietoturvaratkaisun tarkoituksena on olla kokonaisvaltainen ratkaisu, jonka avulla koko organisaation tietoturva voidaan järjestää aina tietoverkon turvaamisesta mobiililaitteisiin, sovelluksiin ja loppukäyttäjiin saakka.



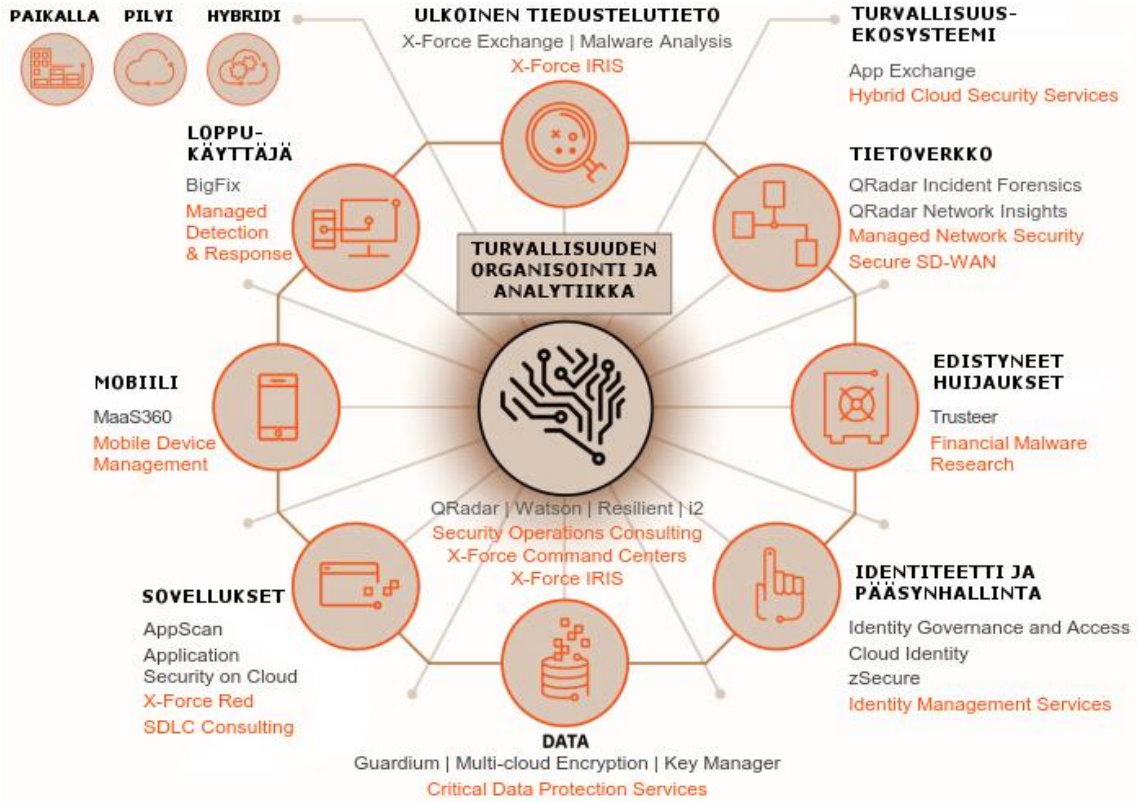
Kuva 31 IBM Security - Integroitu kyberturvallisuuskonsepti (Holm, 2018)

Kuviosta 32 havainnollistuu IBM Security Immune System-ratkaisuun liittyvät sovellukset. Vuonna 2017 Watson for Cyber Securityn kognitiiviset teknologiat integroitiin osaksi uutta IBM Cognitive SOC (Security Operations Consulting) –alustaa, joka antaa tietoturva-asiantuntijoille mahdollisuuden toimia entistä nopeammin ja tarkemmin uhkia vastaan. Alustan keskeisenä sovelluksena on IBM QRadar Watson Advisor, joka hyödyntää ensimmäistä kertaa Watsonin opettamiseksi kerättyä tietoa tietoturvakorpusta. IBM QRadar Watson Advisor ja sen sisältämät kognitiiviset kyvykkyydet ovat asiantuntijoiden hyödynnettävissä IBM QRadar Security Intelligence Platformin kautta. Potentiaalisten uhkien tunnistamiseksi voidaan hyödyntää Watsonin luonnollisen kielen ymmärtämisen

kyvykkyyksiä, jolloin muun muassa blogien, verkkosivujen, tutkimusraporttien ja QRadarin tarjoaman datan läpikäynti helpottuu ja nopeutuu. Prosessi voi nopeuttaa tietoturvauhan selvitykseen kuluvaa aikaa viikoista ja päivistä minuutteihin. IBM SOC –alusta kykenee lisäksi hyödyntämään IBM:n i2-analytiikkatyökalua ja IBM X-Force Exchange-tietokantaa. Tulevaisuudessa asiantuntijoiden avuksi on tietoturvan valvontakeskuksiin tarkoitus kehittää puhuva assistentti, joka kykenee vuorovaikutteiseen toimintaan ja avustamaan tietoturva-analyytikoita muun muassa reaaliaikaisissa tietoturvauhkapäivityksissä ja suosituksien antamisessa uhkatilanteiden korjaamiseksi. Lisäksi IBM Watson voi auttaa tietoturva-asiakkaita, mikäli he haluavat kysyä lisäinformaatiota tietoturvaan liittyvistä asioista chatbot-palveluiden kautta. (Watson for Cyber Security, 2017)

Ulkoisen tiedustelutiedon hallintaan on tarjolla ovat X-Force Exchange-alusta. X-Force Exchange on yhteistyöalusta, joka tuo uhkien analytiikkapalveluita- ja teknologioita pilvipalveluun SaaS (Software as a Service) palveluna nopeuttaakseen yritysten valmiuksia priorisoida uhkia sekä lisätäkseen joustavuutta ja ammattiosaamista. IBM Exchangen käyttäjät voivat hyödyntää IBM:n tietoturva-aineistoa sekä jäsenten että IBM:n asiantuntijoiden tietotaitoa. Tietoturvauhkien tutkimiseksi ja estämiseksi, IBM:n on lisäksi perustanut tietoturva-alan ammattilaisista koostuvan X-Force IRIS (Incident Response and Intelligence Services) -ryhmän, jonka tarkoituksena on vahvistaa asiakasorganisaatiota yhä kehittyviä globaaleja tietoturvauhkia vastaan. (XForce Exchange, 2015)

IBM Security-ratkaisun tietoverkko-osa-alueeseen kuuluvat QRadar Incident Forensics ja QRadar Network Insights sekä Management Network Security Secure ja Secure SD-Wan-palvelut. QRadar Incident Forensics tarjoaa tietoturva-asiantuntijoille mahdollisuuden askel askeleelta jäljittää potentiaalisen hyökkääjän toimia, ja nopeasti sekä helposti toteuttaa tutkimuksia epäilyjä aiheuttavista ja mahdollisesti haitallisista tietoverkkoihin kohdistuvista tapahtumista. QRadar Incident Forensics myös nopeuttaa QRadarin keräämän informaation tutkimista ja prosessi voi nopeutua päivistä tunteihin tai jopa minuutteihin. (IBM QRadar Incident Forencics) QRadar Network Insights analysoi tietoverkossa liikkuvaa dataa reaaliajassa paljastaakseen hyökkääjän ”jalanjäljet” ja paljastaakseen piilossa olevia tietoturvauhkia, esimerkiksi haittaohjelmia, ennen kuin ne vahingoittavat organisaatiota (IBM QRadar Network Insights). Managed Network Security Services tarjoaa monitorointi-, hälytys-, ja verkon tietoturvateknologiapalveluita osana IBM Security-ratkaisua. Palveluiden tarkoituksena on vahvistaa organisaation informaatioturvallisuutta ja laskea kustannuksia (Managed Security Services).



Kuva 32 IBM Security sovellustasolla (Holm, 2018)

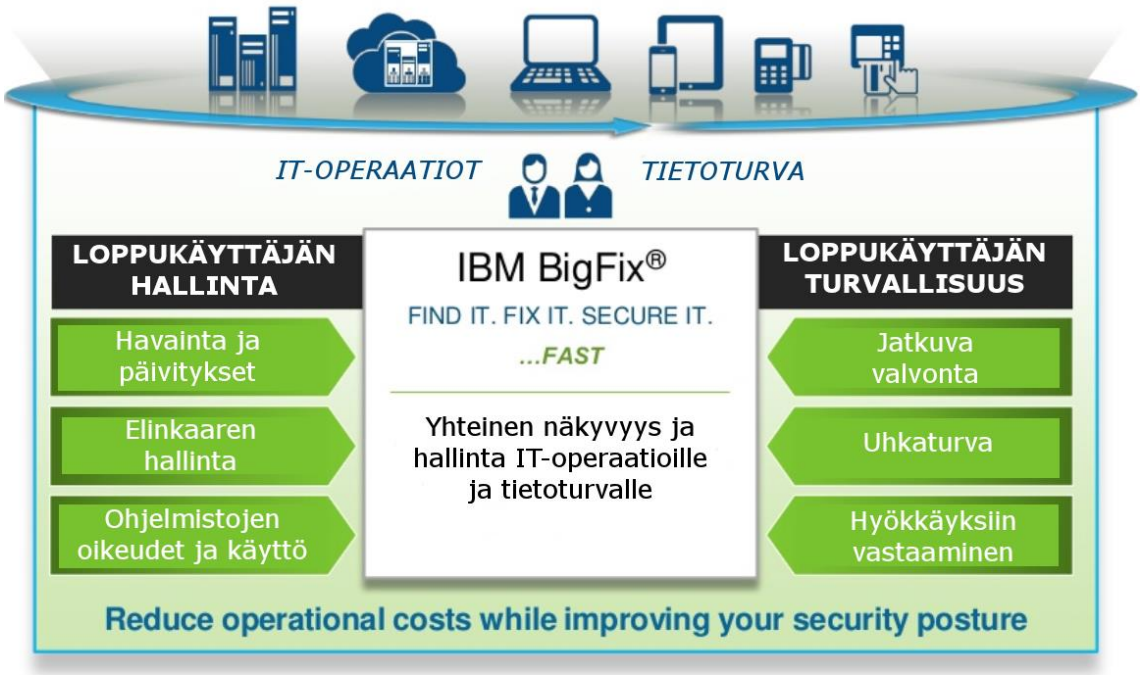
3.10.1 IBM BigFix

IBM BigFix (IBM Endpoint Manager) on IBM:n kehittämä järjestelmähallintaa varten kehitetty alusta, jonka avulla on mahdollista hallita suuria ryhmiä tietokoneita, joiden käyttöjärjestelminä on esimerkiksi Windows, Mac OS X, VMaware ESX, Linux ja Unix sekä erilaiset mobiilikäyttöjärjestelmät, kuten Windows Phone, Symbian, iOS ja Android. IBM BigFix tarjoaa järjestelmän ylläpitäjille työkalut etähallintaan, päivitykseen, ohjelmistojen jakeluun, käyttöjärjestelmien kehitykseen, tietoverkkojen tietoturvan ylläpitämiseen ja laitteistojen sekä ohjelmistojen luetteloimiseen.

BigFix:n alusta jakautuu kahteen (Kuvio 33) alueeseen: IT-operaatioihin ja tietoturvaan sekä edelleen komponentteihin, jotka sisältävät hallinnan (engl. endpoint management) ja tietoturvan (engl. endpoint security). Endpoint management koostuu kolmesta komponentista, jotka ovat ”discovery and patching”, ”lifestyle management” ja “software compliance and usage”. Endpoint security sisältää myös kolme komponenttia, jotka ovat “continuous monitoring”, “threat protection” ja “incident response”.

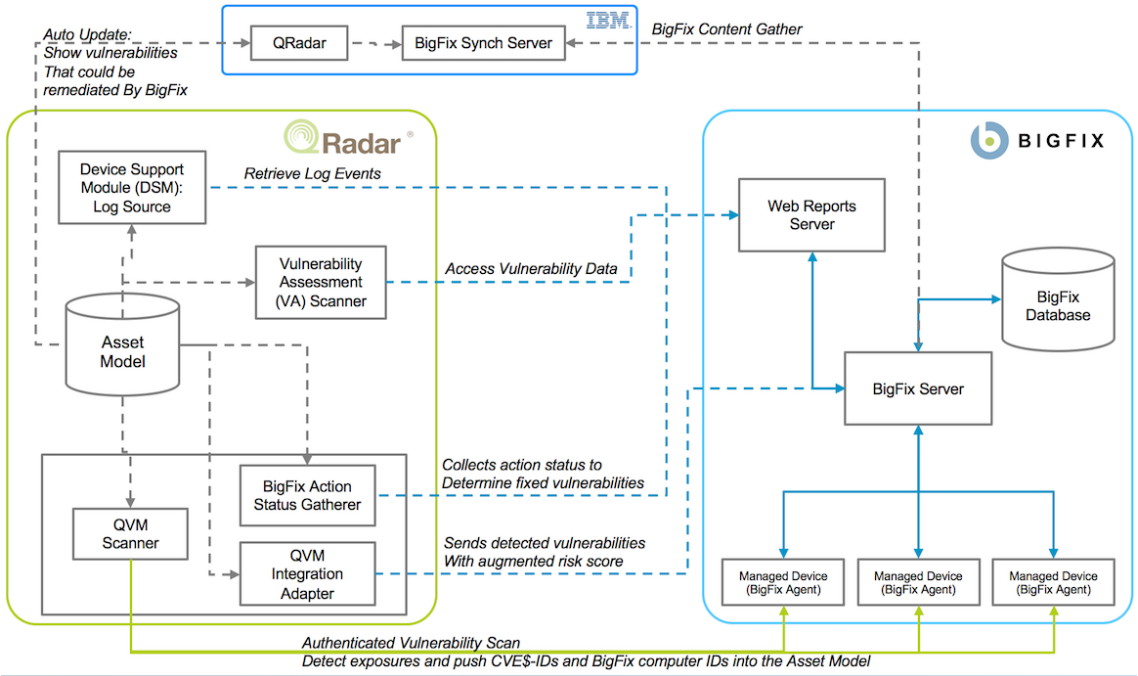
Discovery patching tarjoaa yhden konsolin hallintajärjestelmän useiden laitteiden ja ominaisuuksien identifiointiin, ylläpitoon ja raportointiin. Hallintajärjestelmän avulla voidaan yltää peräti 98 % tulokseen päivitysprosessin onnistumisessa. Lisäksi järjestelmä tuo ajankohtaista tietoa päivitysprosessin tilasta. Lifecycle Management auttaa etsi-

mään ja korjaamaan ongelmia kaikilla alueilla, kuten mobiiliympäristössä, fyysisessä ympäristössä tai virtuaalisessa ympäristössä. Järjestelmän avulla voidaan tarkastaa yli 90 erilaisen käyttöjärjestelmän toimintakyky ja varmistaa, että kaikki päivitykset ovat asennettuina ja tietoturvallisia. Käyttöjärjestelmiin kohdistuvia toimenpiteitä voidaan skriptien avulla automatisoida ja myös haitallisten tiedostojen etsintä voidaan automatisoida. Software compliance and usage auttaa tunnistamaan, mitä ohjelmistoja on asennettuina ja miten niitä käytetään. Toiminnon avulla voidaan löytää kaikki lisensioidut ja lisensioimattomat ohjelmistot. Toiminto auttaa myös pienentämään ohjelmistolisenssien kustannuksia eliminoimalla käyttämättömiä tai tarpeettomia ohjelmistoja. Continuous monitoring tarjoaa ominaisuuksia haavoittuvuuksien etsimiseen ja sisäiseen valvontaan jo ennen hyökkäyksen tapahtumista. Threat protection mahdollistaa reaaliaikaisen hyökkäyksien tunnistuksen ja järjestelmän puolustuksen hyökkäyksien aikana. Hyökkäyksien jo tapahduttua incident response saattaa epäyhteensopivat tai infektoituneet laitteet karanteeniin ja korjaa hyökkäyksistä aiheutuneet infektiot. (Choilawala ym., 2015)



Kuva 33 IBM BigFix IT-operaatiot ja tietoturva (Choilawala ym., 2015)

IBM BigFix- ja QRadar-ohjelmistoja voidaan käyttää yhdessä siten, että IBM QRadar generoi havaitsemiaan tietoturvauhkiin liittyviä hälytyksiä BigFix:n korjattavaksi ja BigFix kehoittaa organisaation IT-tukea korjaamaan haavoittuvuudet. Prosessi parantaa tietoturvauhkien ja haavoittuvuuksien priorisointia, riskien arviointia ja vaatimusten mukaista raportointia. Kuviossa 34 on kuvattuna BigFix-QRadar integraation arkkitehtuurikaavio. BigFix-ohjelmisto toteuttaa haavoittuvuusskannauksia useille erilaisille laitteille ja skannauksien tulokset tallennetaan BigFix-palvelimen kautta BigFix-tietokantaan. BigFix-synkronointipalvelin hakee tietokannan tiedot ja synkronoi ne QRadar-ohjelmistosta tulevan informaation kanssa, jolloin tietoturvauhkiin voidaan puuttua.

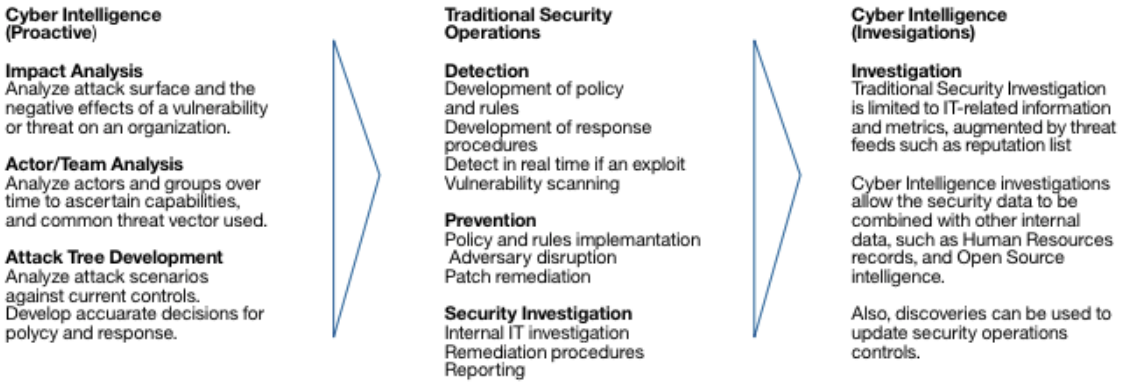


Kuva 34 IBM BigFix-QRadar integraation arkkitehtuurikaavio(Murphy, 2017)

3.10.2 IBM I2 Enterprise Insight Analysis (EIA)

Infrastruktuurin, asiakasyhteyden ja datan turvaaminen ovat kriittisiä asioita liiketoiminnassa ja niin yritysten kuin työntekijöidenkin maineen säilyttämisessä. Kyberhyökkäykset voivat pysyä salassa jopa yli kahdeksan kuukauden ajan ja aiheuttaa yritykselle yli 11 miljoonan Yhdysvaltain dollarin kustannukset. Nykyajan kyberaktoreista on tulossa yhä kehittyneempiä, ketterämpiä ja kykenevämpiä läpäisemään lähes minkä tahansa tietoverkon tietoturvan, jolloin yritysten tulee kehittyä ja korvata perinteisiä tietoturvastrategioita proaktiivisella tietopohjaisella ratkaisulla. Ratkaisu auttaa yrityksiä kriittisesti tarkastelemaan niihin kohdistuvia tietoturvauhkia ja kyberaktoreita. Tämä antaa yrityksille mahdollisuuden kohdata enemmän uhkia moniulotteisen visuaalisen analysointikyvyn ja kehittyneen analytiikan avulla. Lisäksi kyseistä ratkaisumallia hyödyntämällä voidaan myös mahdollisuuksien mukaan vähentää yrityksiin kohdistuneita tietoturvauhkia.

IBM i2 Enterprise Insight Analysis-tietoturvaratkaisun avulla organisaatiot voivat proaktiivisesti saavuttaa kattavan ymmärryksen organisaation haavoittuvuuksista ja kehittää kyberhyökkäysskenaarioita, jotka nopeuttavat hyökkäyksiä koskevien selvityksien ja korjauksien tekemistä. Tulevaisuudessa tapahtuvien hyökkäyksien ehkäisemiseksi, organisaatiot voivat koettaa tunnistaa ja tutkia kyberhyökkääjien toimia hyökkäystapahtumien jälkeen sekä päivittää saadun informaation perusteella kyberturvallisuusstrategiaansa ja taktiikkaansa. Perinteisten tietoturvallisuuteen liittyvät operaatioden ollessa rajoittuneita IT-pohjaiseen dataan ja metriikoihin, proaktiivinen cyber intelligence tarjoaa mahdollisuuden yhdistää dataa muuhun sisäiseen dataan, kuten HR-tietokantoihin, sekä kyberaktoreiden ja ryhmien analysoinnin. Traditionaalista ja proaktiivista cyber intelligenceä on verrattu kuviossa 35. (Cyber Threat Hunting, 2018)

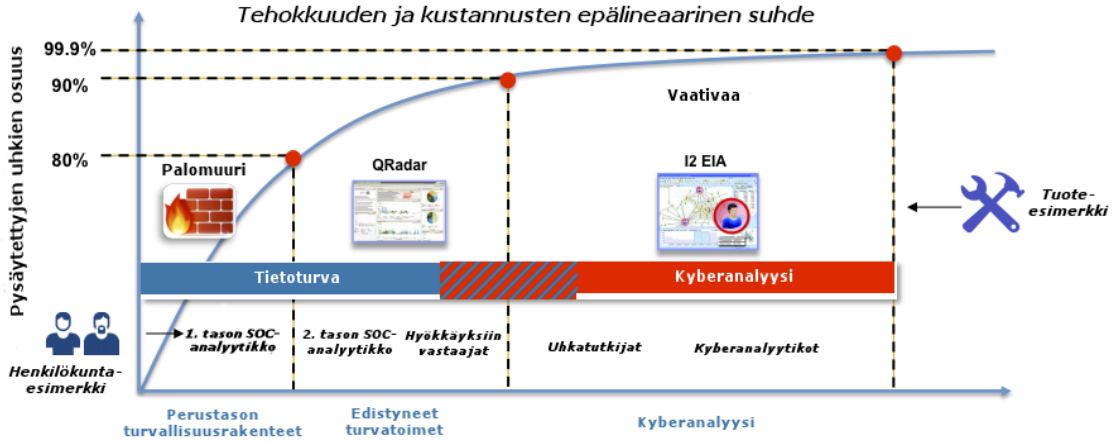


Kuva 35 Traditionaalisen ja proaktiivisen cyber intelligencen vertailua (Cyber Threat Hunting, 2017)

IBM i2 Enterprise Insight Analysis käyttää jo olemassa olevaa tietoturvainfrastruktuuria, muuta infrastruktuuridataa ja avointa lähdekoodia hyödyntävien järjestelmien tarjoamaa dataa. Tietomurron, sen metodien ja tietomurtoon liittyvien tietomurron tekijän henkilökohtaisten tapahtumien tunnistaminen ja tutkiminen perustuvat näiden useiden tietolähteiden hyödyntämiseen. Ratkaisu käyttää myös sosiaalisesta mediasta saatua kerroksittaista dataa, jotta on mahdollista selvittää, kuka on organisaatioon hyökkäävä taho, hänen/heidän sijaintinsa, kohteensa ja kumppaninsa. Näihin tietoihin perustuen organisaatio voi omaksua uusia toimintatapoja ja puolustusta koskevia strategiamuutoksia.

IBM i2 EIA kykenee laajentamaan jo olemassa olevaa tietoturvaratkaisua lisäominaisuuksilla, kuten esimerkiksi visualisointikyvykkyydet. Näitä kyvykkyyksiä voivat olla moniulotteinen visuaalinen analytiikka, jonka avulla tutkijat voivat saada paremman kuvan hyökkäyksestä visualisoimalla kattavan tilannekuvan kaikista tilanteeseen liittyvistä elementeistä. EIA:n avoin ja modulaarinen arkkitehtuuri on skaalautuva ja lisäksi täysin räätälöitävissä kolmannen osapuolen sovelluksien ja niiden tarjoamien ominaisuuksien kanssa, kuten luonnollisen kielen prosessointi, sekä analytiikka taktisella, operationaalisella ja strategisella tasolla. EIA tarjoaa myös yhteensopivuuden organisaation sisällä ja ulkopuolella. Avoin malli ei pelkästään integroi jo olemassa olevaan arkkitehtuuriin ja muihin sovelluksiin, vaan antaa käyttäjille mahdollisuuden helposti jakaa informaatiota tietoturvauhkista organisaation laajuisesti sekä kumppaneiden, asiakkaiden ja muiden organisaatioiden kanssa. (Audet, 2014)

Perinteinen palomuuri kykenee kuviossa 36 esitetyn käyrän mukaisesti ehkäisemään maksimissaan 80 % kyberhyökkäyksistä. IBM:n QRadarin tuoma lisäarvo traditionaalisen palomuurin käyttöön on 0-10 % yksikköä, jolloin on mahdollista saavuttaa 90 % taso. IBM:n EIA, joka hyödyntää kyberanalyysia vaatien eniten käytännön työtä, lisää turvallisuutta edelleen ja sen avulla on mahdollista saavuttaa jopa 99.9 % taso. Kyberanalyysia tekevät kyberuhkien tutkijat ja analyytikot.

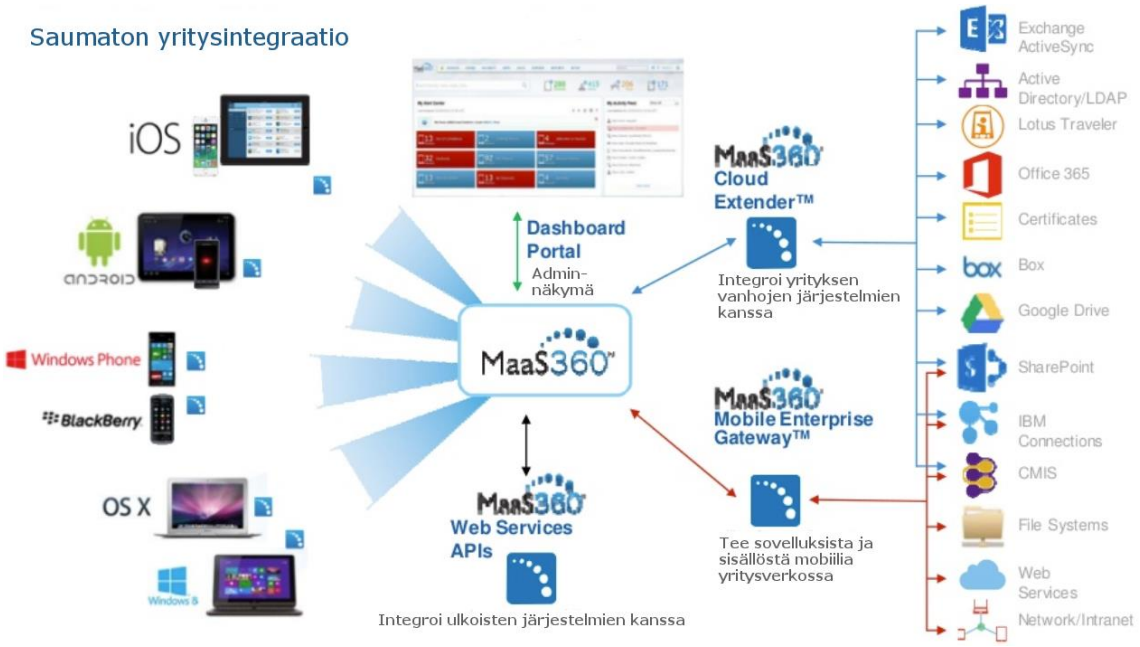


Kuva 36 Traditionaalinen informaatioturvallisuus ja kyberanalytiikka (Stasio, 2015)

3.10.3 IBM MaaS360 with Watson

IBM MaaS360 on IBM:n kehittämä mobiililaitteiden hallintasovellus, joka mahdollistaa kaikkien organisaation mobiilien henkilökohtaisten laitteiden, sovelluksien ja sisällön hallinnan ja tietoturvan ilman, että se verottaa IT-tuen resursseja. MaaS360 tarjoaa tietoturvallisen ympäristön, joka pitää yrityksen mahdollisia liikesalaisuuksia sisältävät tiedostot erossa mobiililaitteeseen asennetuilta sovelluksilta. Tämä mahdollistaa sen, että organisaatioiden työntekijät voivat työskennellä vaarantamatta sekä dataan että laitteeseen liittyvää tietoturvaa. Ratkaisu yksinkertaistaa IT:n hallintaa, sillä on tarpeen monitoroida ainoastaan ympäristöä kontrolloivaa sovellusta, eikä koko laitetta. (IBM MaaS360)

MaaS360 tarjoaa organisaation IT-osastolle yksinkertaisen tavan hallita mobiilaitteita (Kuvio 37). Sovelluksen avulla, kaikkia laitteita voidaan monitoroida yhdestä paikasta ja valvoa langattomasti. MaaS360:n tarjoaman mobiilalaitteiden hallintakyvyn yritykset aina pienyrityksistä suuriin asti voivat antaa työntekijöille mahdollisuuden käyttää työtehtäviensä toteutuksessa heidän omia mobiilaitteitaan. Omien henkilökohtaisten mobiillaitteiden hyödyntäminen työtehtävien hoidossa voi nostaa työntekijän tuottavuutta, sillä silloin he voivat työskennellä laitteilla, jotka tuntuvat heille kaikkein tutuimmalta ja lisäksi ilman pelkoa tietoturvan vaarantamisesta. (IBM MaaS360)



Kuva 37 Traditionaalisen ja proaktiivisen cyber intelligencen vertailua (Cyber Threat Hunting, 2017)

MaaS360:n avulla organisaatiot voivat hallita sovelluksia interaktiivisen luettelon välityksellä, jonka kautta ne voivat rohkaista käyttämään valittuja sovelluksia, jakaa niitä käyttäjille ja päivittää niitä tarpeen vaatiessa. Lisäksi MaaS360 varmistaa, että yrityksen data on salattuna ja että se pidetään erillään muista mobiililaitteisiin asennetuista sovelluksista, jotta ne eivät pääse siihen käsiksi. Menettely säästää arvokkaita resursseja ja lisäksi rakentaa luottamusta työntekijöiden ja organisaation IT-yksikön välille. MaaS:n avulla organisaatiot voivat myös rajoittaa työntekijöiden oikeuksia dataan ja sallia heille oikeuksia, joita he tarvitsevat työtehtäviensä hoitamiseksi, mutta hyvin kontrolloidusti. Lisäksi ympäristö tarjoaa kalenteriominaisuuden tapaamisten sopimiseksi ja reaaliaikaisen chat-keskusteluominaisuuden. (IBM MaaS360)

Kuten edellä mainittiin, MaaS360 sisältää tietynlaisen datan hallintaa ja tallennusta varten toteutetun tietoturvallisen säiliön (enlg. container), joka auttaa varmistamaan, että data on varastoituna mobiililaitteella, eikä palvelimilla, jolloin palveluntarjoajien IT-palveluissa työskentelevät henkilöt eivät voi tarkastella sitä. Lisäksi säiliön avulla voidaan varmistaa, että oikeuksia datan käsittelyyn säädellään tarveperusteisesti. Data on salattuna AES-256 CTR-salausalgoritmilla, CommonCrypto FIPS 140-2-yhteensopivalla algoritmilla (Applen laitteet) tai SQLCipher + OpenSSL (AES-256) salausalgoritmilla, mikäli käytössä on Android-laitteita. Ohjelmisto huomioi myös GDPR-vaatimukset. (IBM_B)

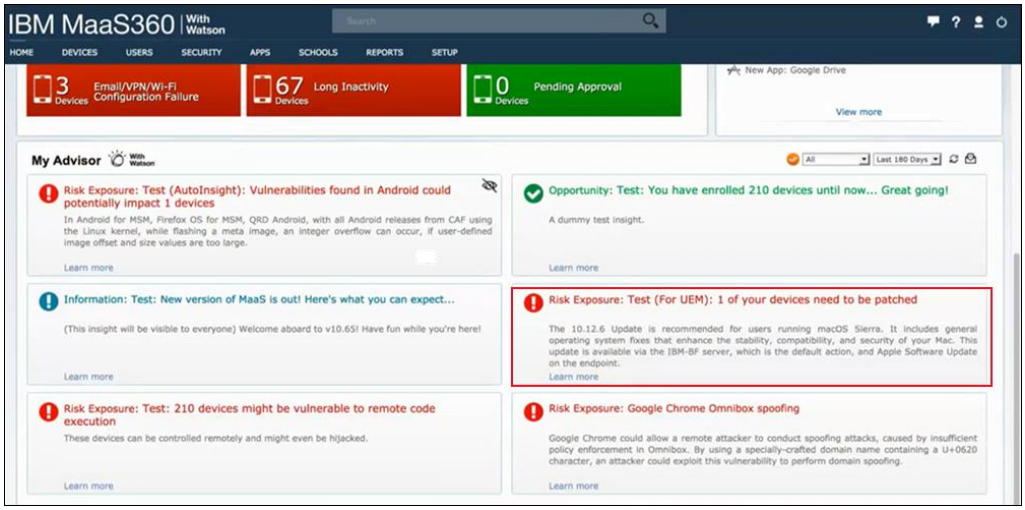
MaaS360-ominaisuuksia ovat muun muassa (IBM MaaS360):

- Laitteiden etähallinta
- Sovellusten etähallinta
- Interaktiivinen sovellusluettelo
- Nopea sovellusten käyttöönotto
- Sisältöyhteistyö
- Reaaliaikainen dokumenttien vaihdon ilmoitus
- Tietoturvalliset sovellukset ja data
- Organisaation tietojärjestelmien integrointi
- Henkilökohtaisten mobiililaitteiden käytön mahdollistaminen
- Yksinkertainen laitteiden rekisteröinti
- Mobiilien haittaohjelmien ongelmanratkaisu
- Laitteiden käyttöoikeuksien peruutusominaisuus

Ehkä yksi tärkeimmistä MaaS360:n ominaisuuksista on IBM Watsonin tarjoama kognitiivinen analytiikka, jolloin historiatietoja, nykyisyyden tietoa sekä tulevaisuuden ennusteita hyödyntäen voidaan parantaa päätöksentekoprosessia ja auttaa IT- sekä tietoturvallisuusjohtajia EU:n tietoturva-asetuksen GDPR:n (General Data Protection Regulation) huomioinnissa (IBM_B). MaaS360 with Watsonin analytiikkaominaisuudet sisältävät seuraavanlaisia kyvykkyyksiä:

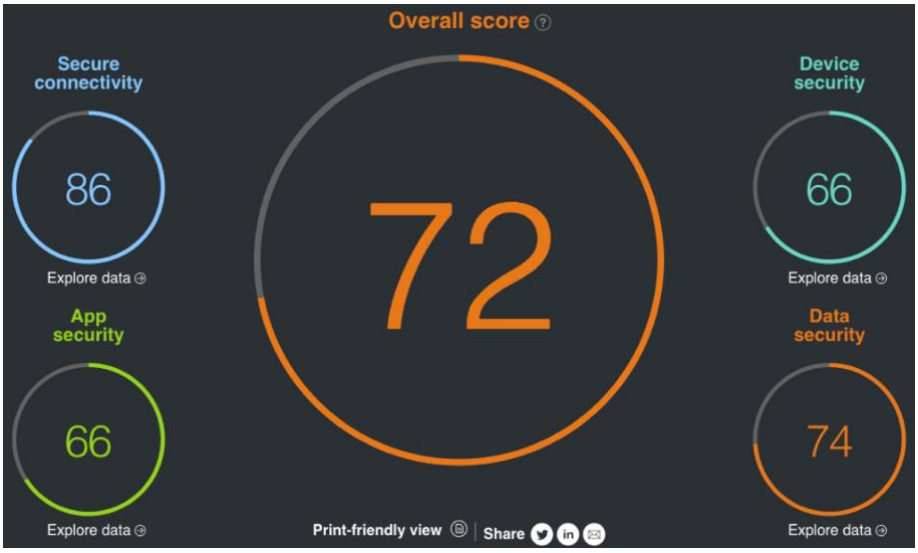
- **Advisor**: Tuottaa relevanttia hyödynnettävää informaatiota rakenteellisesta ja rakenteettomasta organisaation datasta.
- **Mobile Security Index**: Tarjoaa julkisesti avoimen mobiilin tietoturvan tulostaulukon.
- **Mobile Metrics**: Tarjoaa pilvipohjaisen datan suorituskykytestin ja parhaat käytänteet tuottavuuden laajentamiseksi ja tietoturvan maksimoimiseksi.

Maas360 Advisorin ytimessä on tehokas kognitiivinen moottori, joka tarjoaa informaatiota relevanteista hälytyksistä (Kuvio 38) koskien syntymässä olevia tietoturvauhkia. Tämä informaatio perustuu sekä rakenteelliseen että rakenteettomaan dataan ja on spesifistä organisaation teollisuudenalalle, koolle ja mobiiliympäristölle. Advisorin avulla organisaatiot kykenevät löytämään parhaat käytänteet työntekijöiden tuottavuudelle, suositukset IT-palveluiden optimoinnille ja lisäksi informaatiota potentiaalisista tietoturvauhkista. Informaatio näytetään MaaS360:n dashboard-näkymässä. Informaation avulla voidaan muun muassa arvioida tietoturvauhkien vaikutusta organisaation laitteistoihin, käyttäjiin ja sovelluksiin, ja valita paras tapa korjata ongelma.



Kuva 38 MaaS360 Advisor with Watson (Stasio, 2015)

IBM MaaS360 Security Index on teollisuuden ensimmäinen julkisesti saatavilla oleva mobiilin tietoturvan tuloskortti (Kuvio 39).



Kuva 39 MaaS360 Security Index-tuloskortti. (Stasio, 2015)

3.10.4 IBM Mainframe Security

Keskuskoneiden (mainframe) tultua 1960-luvulla tietoverkot olivat vielä pieniä ja hyvin määriteltyjä. Niiden käyttäjiä oli vähän ja he olivat tunnettuja koko organisaatiossa. Organisaation tietoverkkoon päästäkseen henkilön tuli olla organisaation tiloissa ja usein lisäksi virka-aikana. Fyysinen data saattoi olla varkauksille, haitanteolle tai tuhoamiselle alttiina. Luvattoman käyttäjän päästessä järjestelmään, järjestelmään tallennettu informaatio oli tyypillisesti rajoittunut transaktioihin ja eräkäsittelyinformaatioon (batch processing). Nykyään keskuskoneet ovat yhteydessä Internetiin, joka ulottuu kaikkialle maailmaan. Käytännössä kaikilla luvallisilla käyttäjillä on pääsy henkilökohtaisten tietokoneiden ja mobiililaitteiden välityksellä keskuskonepohjaisiin WEB-palvelimiin. Organi-

saatiot tallentavat aineetonta omaisuuttaan ja kriittistä liiketoimintadataa keskuskoneille tarjoten otollisen alustan taloudellista etua tavoitteleville hyökkääjille. (Thought Leadership White Paper, 2013)

Keskustietokoneiden sisältäessä useita sisäänrakennettuja tietoturvakyvykkyyksiä, niihin kohdistuu suhteellisen harvoin onnistuneita hyökkäyksiä. Tutkimuksien mukaan vain yksi prosentti hyökkäyksistä onnistuu. Organisaatioille haasteita aiheuttavat tietoturvauhkien muuttuva luonne ja keskustietokoneiden tietoturvan pitäminen ajan tasalla. Tietoturvauhkien ja niiden vakavuusasteiden lisääntyessä, useat organisaatiot ovat keskittäneet resurssinsa haavoittuvampien alustojen suojaamiseen. Organisaatiot voivat lisäksi virheellisesti uskoa, että keskustietokone, jonka tietoturva oli ajan tasalla muutama vuosi sitten, on sitä edelleen nykyään. Keskustietokoneiden toimintaympäristöt monimutkaistuvat jatkuvasti ja ne ovat yhä vaikeampia ylläpitää sekä yhä haavoittuvampia hyökkäyksille. Heikosti konfiguroitu järjestelmä voi olla hyökkääjän kohteena, vaikka kyseessä olisi keskustietokone. Samanaikaisesti keskuskonejärjestelmän käyttöaste kasvaa ja yhä kasvava etäkäyttäjien joukko rajoittaa sisäisten palveluiden kontrollointimahdollisuuksia. Mobiilikäyttäjien ja heille tarjottujen palveluiden lisääntyminen lisäksi avaa yhä enemmän tilaisuuksia hyökkääjille. (Thought Leadership White Paper, 2013)

Jopa maailman tietoturvallisimmat laskenta-alustat, kuten muukin IT-infrastruktuuri, tarvitsevat sekä suojausta tietoturvauhkia ja –murtoja vastaan sekä kykyä vastata nopeasti teollisuuden ja hallituksen sääntelyihin. Ne tyypillisesti varastoivat organisaation kriittiisintä data, jolloin keskustietokonealustat, kuten IBM System Z, ovat hyökkääjien ja sisäisten tietomurtojen kohteena. IBM:n System Z-alusta on suunniteltu tämänkaltaisiin tietoturvauhkiin vastaamiseen ja se on suunniteltu tarjoamaan ennakoiva suojautumislähestymistapa organisaatioiden infrastuktuuria ja informaatiota varten. System Z-alustaa ja z/OS-käyttöjärjestelmää pidetään eräänä turvallisimmista kaupallisista saatavilla olevista käyttöjärjestelmistä ja System Z on läpikäynyt tiukkoja sertifiointiprosesseija niin traditionaalisissa z/OS-ympäristöissä kuin virtuaalisissa ympäristöissä. System Z on myös EAL5+-arvioitu, joka on korkein keskustietokoneympäristöille toteutettava arviointi. Lisäksi se on saavuttanut Federal Information Processing Standardissa (FIPS) 140 pistettä, jonka on myöntänyt National Institute of Standards and Technology (NIST). (Thought Leadership White Paper, 2013)

IBM:n ZSecure-ratkaisu (Kuva 40) on suunniteltu auttamaan loppukäyttäjiä hallitsemaan keskustietokoneiden tietoturvallisuutta, monitoroimaan tietoturvauhkia, valvomaan käyttöä ja konfigurointeja sekä valvomaan sääntöjen noudattamista. ZSecure parantaa keskustietokoneiden tietoturvaympäristön tehokkuutta ja hallittavuutta, jolloin sen avulla voidaan laskea kustanuksia, tehostaa tuottavuutta, hyödyntää hajautettua hallintoa ja nopeuttaa vasteaikoja liiketoiminnan tukemiseksi. Valvonnan ja monitoroinnin automatisointi sekä sääntöjen mukaan toimiminen voi auttaa organisaatioita parantamaan tietoturvaa ja tietoturvatapauksien käsittelyä sekä parantamaan operatiivista tehokkuutta kustannusten ja riskien laskemiseksi. ZSecure-ratkaisu tarjoaa työkaluja aina hyökkäysten tunnistamisesta ja estämisestä väärien konfiguraatioiden tunnistamiseeen reaaliaikaista monitorointia hyödyntäen. Lisäksi ratkaisun avulla voidaan toteuttaa kattavia data-analyysejä, joiden avulla voidaan tunnistaa piilossa olevia ja monimutkaisia

riskejä, tehdä hälytyksiä ja räätälöityjä raportteja. (Thought Leadership White Paper, 2013)

ZSecure-ratkaisuun kuuluu oleellisena osana jo vuonna 1976 julkaistu **RACF** (Resource Access Control Facility) tietoturvajärjestelmä, joka tarjoaa käytön hallinnan ja valvonnan toiminnallisuuksia Z/OS- ja z/VM käyttöjärjestelmille. RACF:n avulla organisaatiot voivat kontrolloida ja määritellä ratkaisun käyttöön oikeutettujen käyttäjien profiileita, tehdä käyttöön liittyviä päätöksiä ja luoda lokitiedostoja tarkempaa jatkotarkastelua varten. Resurssien suojelemiseksi RACF säilyttää relevanttia informaatiota käyttäjistä, resursseista ja järjestelmän asiantuntijoista. Tätä informaatiota hyödynnetään käyttäjien tunnistamisessa ja pääsyn myöntämisessä suojattuihin resursseihin sekä luvattomien käyttöyrityksien tallentamisessa lokitietoihin. RACF:n avulla voidaan märitellä erilliset käyttäjäroolit tietoturvan hallintaan ja auditointeihin sekä rahoittaa käyttöoikeuksia ryhmittäin. (Thought Leadership White Paper, 2013)

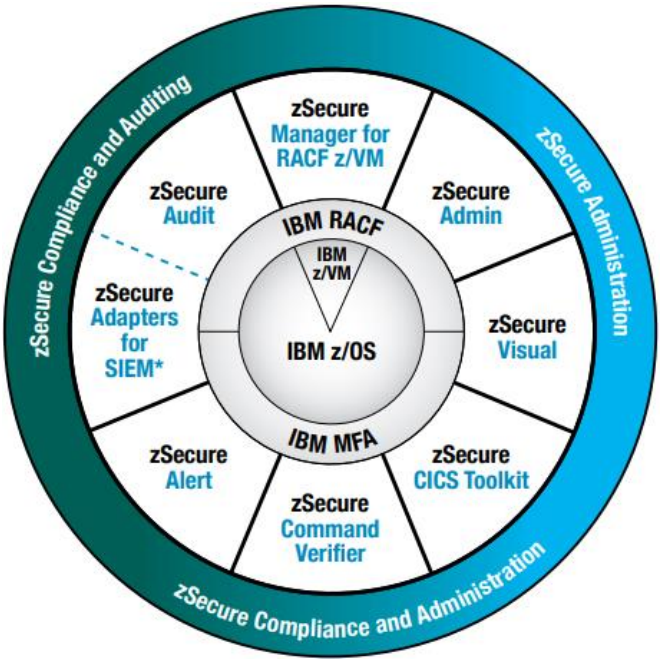
RACF:n pääominaisuuksia ovat:

- Autentikointi, jossa käyttäjä tunnistetaan ja varmistetaan käyttäjä-ID:n ja salasanan tarkastusten avulla
- Järjestelmäresurssien identifiointi, luokittelu ja suojaaminen
- Auktorisointi, jossa ylläpidetään suojatuille resursseille tarkoitettuja käyttöoikeuksia
- Suojattujen resurssien käyttömahdollisuuksien kontrollointi
- Auditointi, jossa suojattujen järjestelmien ja resurssien käyttöä valvotaan

IBM zSecure Administration koostuu **zSecure Admin** ja **zSecure Visual**-työkaluista. zSecure Admin automatisoi ja yksinkertaistaa IBM RACF-tietoturvan hallintatehtäviä sekä laajentaa RACF:n delegointikyvykyyksiä ja identiteetin hallintaa. Automatisoimalla useita toistuvia järjestelmän hallintatehtäviä ja laajentamalla natiivin RACF:n auktorisointi- ja delegointikyvykkyyksiä, **zSecure Admin** kykenee maksimoimaan IT-resurssit, vähentämään virhetilanteita, parantamaan tehokkuutta sekä palvelun laatua ja tunnistamaan ongelmat nopeasti tietoturvariskien minimoimiseksi ja sääntöjen noudattamiseksi sekä pienentämään kustannuksia. Admin automatisoi myös toistuvia tietoturvatehtäviä, kuten salasanojen hallinta ja käyttäjien sekä ryhmien ID-informaation kopiointi ja poistaminen. Admin kykenee myös yhdistämään säännöstöjä (security rules) erilaisista tietokannoista nopeasti ja tehokkaasti sekä pitämään useat eri RACF-tietokannat synkronoituina. Lisäksi Adminin kyvykkyyksiin kuuluu tietokantojen siivoaminen ja käskyjen muodostaminen tehtävän suorittamiseksi. (IBM Security zSecure Admin)

zSecure Visual yksinkertaistaa RACF:n hallintaa Microsoft-pohjaista käyttöliittymää hyödyntäen ja antaa mahdollisuuden RACF:n ylläpitäjille keskittyä vaativimpien tehtävien hoitamiseen. zSecure Visual säästää kustannuksia tarjoten yksinkertaisen RACF:n hallinnan suoraan Microsoft Windows-käyttöjärjestelmätasolta soveltuvia profiileita hyödyntäen. zSecure Visual-käyttöliittymä tarvitsee toimiakseen vähemmän resursseja ja tarjoaa enemmän toiminallisuuksia kuin aiemmat ratkaisut ja käyttöliittymän avulla liiketoimintajohtajat voivat ketterästi tarkastella kriittistä informaatiota koskien henkilöstöä ja resursseja. zSecure Visual optimoi resursseja hajauttamalla RACF:n ylläpidon siten,

että se voidaan toteuttaa osastotasoittain, eikä korporaatiotasolla. ZSecure Administration tarjoaa näkyvyyden koko RACF-infrastruktuuriin, jolloin loppukäyttäjien on mahdollista toteuttaa hallinnollisia toimenpiteitä ja tehdä raportteja yhdestä käyttöliittymästä. Administration parantaa tietoturvaa, auttaa vähentämään virheitä tarjoamalla simulaatio- ja testiympäristöjä sekä auttaa vähentämään työvoimakuluja siivoten automaattisesti käyttämättömiä tilejä ja profiileita. Administration integroituu RACF- ja IBM MFA sekä IBM Operations Analytics for zSystems-ratkaisuihin. (IBM Security zSecure Suite, 2017)



Kuva 40 IBM Mainframe Securityn ratkaisut (IBM Security zSecure Suite, 2017)

IBM Security zSecure Compliance and Auditing koostuu kolmesta ratkaisusta, jotka ovat **IBM zSecure Audit**, **IBM zSecure Alert** ja **IBM zSecure Command Verifier**. Compliance and Auditing-ratkaisu automatisoi tietoturvariskien tunnistuksen, tapahtuma-analyysit ja sääntöjen noudattamisen monitoroinnin riskien pienentämiseksi ja kustannuksien säästämiseksi. Tietoturvariskien tunnistamisessa Compliance and Auditing hyödyntää data-analytiikkaa. zSecure Compliance and Auditing parantaa auditointeja toteuttamalla automaattisia analyysejä hyödyntäen sisäänrakennettua tietokantaa. Ratkaisun avulla voidaan räätälöidä raportoinnit liiketoimintamallin- ja vaatimusten mukaisesti riskejä vähentäen. Compliance and Auditing integroituu IBM QRadar SIEM-, IBM Security Guardum-, RACF-, MFA-, IBM Operations Analytics for z Systems- ja IBM Common Data provider for z System solutions -ratkaisuihin. (IBM Security zSecure Suite, 2017)

IBM zSecure Audit korvaa perinteiset auditointimenetelmät tietoturvariskien ja väärän-laisten konfigurointien automaattisessa tunnistamisessa. Audit mittaa ja verifioi IBM mainframe-tietoturvakäytänteiden tehokkuutta koskien RACF, CA-ACF2 ja CA Top tietoturvaratkaisuja. Audit parantaa auditointien laatua toteuttamalla laajan automatisoidun analyysin käyttöjärjestelmästä, tietoturvajärjestelmästä ja tärkeimmistä alijärjestelmistä hyödyntäen sisäänrakenettua tietokantaa. Audit generoi raportteja, joiden avulla voidaan nopeasti paikallistaa tiettyihin resursseihin kohdistuvia ongelmia, kuten suojaamaton data-aineisto. Tämä mahdollistaa haavoittuvuusanalyysin tarjoamisen koskien keskustietokoneinfrastruktuuria. Ratkaisu tarjoaa lisäksi viitekehyksen teollisuuden säännöstöjen noudattamiseksi. Lopputuloksena virheet voivat vähentyä ja palvelun laatu parantua. Relevanttia tietoturvainformaatiota voidaan lisäksi integroida kriittisistä IBM z/OS-alijärjestelmistä ja sovelluksista, kuten IBM MQ for z/OS, IBM Db2, IBM CICS, IBM z/OS Communications Server (TCP/IP), UNIX, Linux on IBM Z, IBM RACF, CA ACF2 ja CA TP Secret Security. Ratkaisun integroituu RACF, IBM QRadar SIEM, IBM Security Guardum ja IBM Common Data Provider for z Systems-ratkaisuihin tarjoten koko organisation laajuisen analyysin ja kognitiivisen analytiikan palvelut yhteiskäytössä IBM QRadar Advisor with Watson-ratkaisun kanssa. (IBM Security zSecure Audit)

IBM Security zSecure Alert auttaa loppukäyttäjää rakentamaan keskustietokoneiden monitorointijärjestelmän osaksi organisaation tietoturvauhkien monitorointia, jotta organisaatio kykenee monitoroimaan sisäisiä ja ulkoisia tietoturvauhkia sekä väärin toteutettuja konfiguraatioita. zSecure Alert tehostaa auditointia ja tarjoaa tapahtumanhallinnan yksinkertaistaen keskustietokonejärjestelmän ylläpitoa, parantaen järjestelmän saatavillaoloa ja säästäen kustannuksissa. IBM Security zSecure Alert kykenee monitoroimaan kriittistä dataa tarjoten ennalta määritellyt hälytykset, joiden avulla on mahdollista nopeasti tunnistaa sopimattomat toimenpiteet ja loppukäyttäjän käyttäytyminen, jolloin tietoturvatapahtumiin voidaan reagoida nopeammin. zSecure Alert ylläpitää myös datan eheyttä tunnistaen haitallisen toiminnan, vaikka se ei olisi tallentunut tapahtumalokiin. Ratkaisun hyödyntäminen ja automaattinen reaaliaikainen keskustietokonemonitorointi vähentävät kustannuksia ja epäonnistuneita auditointeja. Ratkaisun avulla voidaan myös suorittaa nopeita diagnosointitoimenpiteitä ja vastata tietoturvariskeihin hyödyntäen suljetun silmukan monitorointimenetelmää sekä erilaisten interventio- ja korjaustoimenpiteiden kautta. (IBM Security zSecure Alert)

IBM Security zSecure Command Verifier tarjoaa tietoturvallisen kerroksen, joka antaa käyttäjälle mahdollisuuden verrata jokaista IBM RACF-käskyä organisaation tietoturvapolitiikkaan jo ennen niiden prosessointia. Ratkaisu estää tietoturvamuutokset, jotka voivat heikentää järjestelmien saatavilla oloa, aiheuttaa haavoittuvuuksia ja jotka voivat saastuttaa tietokannat. zSecure Command Verifier monitoroi tietoturvapolitiikan noudattamista. Komennot tulkitaan siten, miten ne on kirjoitettu ja niitä voidaan verrata organisaation tietoturvasäännöstöihin. Tällöin voidaan tehdä päätös, tuleeko niitä suorittaa, vai ei. Command verifier myös vähentää riskejä ja säästää aikaa. Tehdyistä muutoksista voidaan saada informaatiota hyvin nopeasti säästäen jopa tunteja aikaa aiemman lokitiedostojen tarkastelemisen sijasta. Lisäksi ratkaisu vähentää riskejä, joita käyttäjät voivat tahallisesti tai tahattomasti aiheuttaa. Command verifier myös parantaa tietoturvakontrolleita mahdollistamalla fokusoidumpien käskyjen määrittämisen RACF:n

säännöstön mukaisesti. Lisäksi ratkaisun avulla on mahdollista generoida hälytyksiä. IBM Security zSecure Command Verifier integroituu yleisten IBM:n alustojen kanssa, mutta toimii tarvittaessa myös itsenäisesti erillään muista zSecure-ratkaisuista. (IBM Security zSecure Command Verifier)

IBM Security zSecure Adapter for Siem automatisoi ja integroi manuaalisen tapahtuma-analyysin ja monitoroinnin sääntöjen noudattamista varten. Ratkaisu täydentää IBM Security zSecure Alert-ratkaisua, joka lähettää reaaliaikaisia hälytyksiä tietoturvauhkista. Ratkaisu myös integroi ja kerää tietoturvatapahtumia useasta eri IBM z/OS-lähteestä raportointia varten. zSecure Adapter for SIEM hyödyntää data-analytiikkaa ja dashboard-kojelautanäkymiä monimutkaisten ja piilossa olevien tietoturvariskien tunnistamiseksi. Ratkaisu tukee IBM RACF, CA ACF2 ja CA Top Secret järjestelmiä ja integroituu RACF-, IBM QRadar SIEM- ja IBM Common Data Provider for zSystems-ratkaisujen kanssa koko organisaation laajuisen reaaliaikaisen ja kognitiivisen analyysin toteuttamiseksi IBM QRadar Advisor with WatsonTM-ratkaisua hyödyntäen. (IBM Security zSecure Suite, 2017)

IBM Adapter for SIEM muotoilee ja lähettää lähes reaaliajassa keskustietokoneiden järjestelmähallinnan (System Management Facility eli SFM) auditointidataa SIEM-ratkaisuille, kuten IBM QRadar SIEM, joka on koko organisaation laajuisen integroitujen tietojärjestelmien- ja verkkojen poikkeamien tarkkailuun keskittynyt järjestelmä. Lisäksi dataa voidaan hyödyntää lokitiedostojen hallinnassa, anomalioiden tunnistamisessa, tietoturvatapahtumien tutkimisessa, asetuksien tarkastamisessa sekä lisäksi haavoittuvuuksien ja riskien hallinnan alueilla. IBM zSecure Adapter for SIEM voi vähentää tietoturvatapahtumien kustannuksia tukien yli 40 erilaisen IBM System z-ratkaisun SFM-tietotyyppejä. Lisäksi Adapter for SIEM kykenee tehokkaasti hallitsemaan suuria määriä tietoturvatapahtumia. Ratkaisu tarjoaa myös paremman näkymän dataan ja sen avulla on mahdolilsta saada kattavaa ja yksityiskohtaista auditointi-informaatiota käyttäjistä ja resursseista käyttäen älykkäitä suodattimia, nimen perusteella tunnnistamista, käyttöoikeuksia ja muuta tietoturvainformaatiota. (zSecure Improves Security Information and Management)

IBM Security zSecurity CICS Toolkit automatisoi ja keskittää tietoturva-auktorisoinnit sovelluksista IBM RACF-ratkaisuun, joka toimii tietoturvaa hallinnoivana ratkaisuna hyödyntäen tietoturvaominaisuuksia, joita on sisäänrakennettu IBM z/OS-käyttöjärjestelmään. CICS Toolkit kykenee tunnistamaan potentiaalisia heikkouksia sovellusten pääsykontrolleissa (engl. access control) ja auditoinneissa RACF-ratkaisua hyödyntäen. CICS hyödyntää RACF-ratkaisua identiteetin ja pääsyn hallinnassa, jolloin kyseisiä ominaisuuksia ei tarvitse rakentaa osaksi CICS-ratkaisua. CICS näyttää käyttäjälle ainoastaan niitä toimintoja ja vaihtoehtoja, jotka on määritelty käyttäjille CICS Toolkit-käyttöliittymän kautta. Tämä auttaa osaltaan virhetilanteiden vähenemisessä. zSecurity CICS Toolkit myös auttaa parantamaan vanhempien sovellusten tietoturvaa toteuttamalla autentikointi- ja auktorisointitarkastuksia. Lisäksi CICS auttaa pienentämään sovelluskehityksen ja ylläpidon kustannuksia, parantamaan tuottavuutta ja helpottamaan tietoturvan hallintaa. CISC Toolkit integroituu RACF-ratkaisun kanssa. (IBM Security zSecure Suite, 2017)

IBM CICS-toolkit tarjoaa keskustietokoneen ylläpitokyvykkyysiä, kuten salasanan resetonnin ja luvanhallinnan CICS-ympäristöön. Ohjelmisto tarjoaa ylläpitäjille joustavuutta lupien hallinnan toteutukseen CICS-transaktioita hyödyntäen. Käyttöliittymä näyttää ainoastaan ne toiminnot ja ominaisuudet, joihin käyttäjä on valtuutettu. CICS-toolkit auttaa tehostamaan tuottavuutta ja vähentämään kehitystyöhön kuluvaa aikaa, sillä sovellusohjelmoijien ei tarvitse tuntea IBM:n RACF-tietokantaa, jotta he voivat kehittää räätälöityjä tietoturvasovelluksia. CICS-toolkit mahdollistaa myös API-rajapintaa hyödyntäen näkymien räätälöinnin ja informaation kontrolloinnin tietyn asennuksen vaatimusten mukaisesti. (IBM Security zSecure CICS Toolkit)

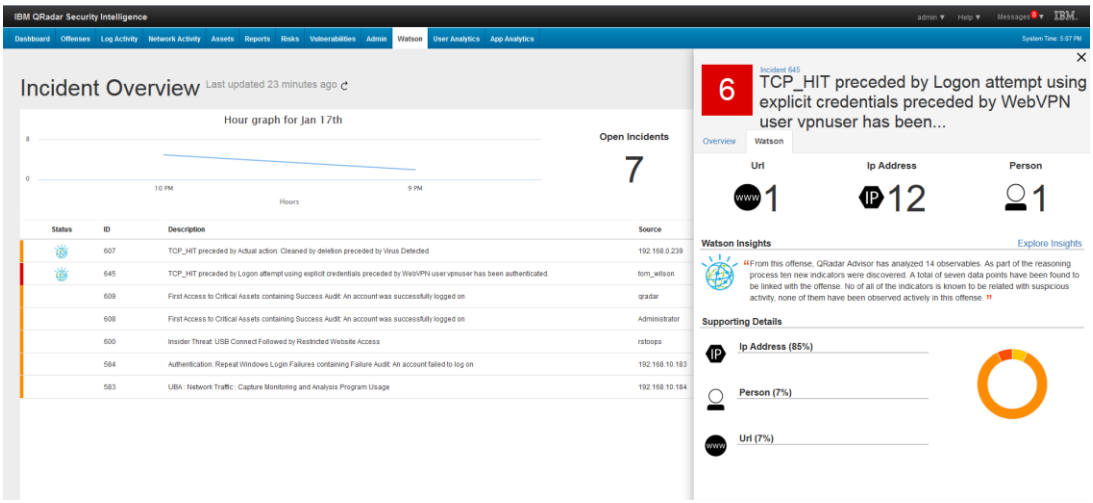
IBM Multi-Factor Authentication for z/OS (IBM MFA) suojaa käyttäjiä vaatimalla useita autentikointifaktoreita, jotka osaltaan nostavat organisaation tietoturvan tasoa. IBM MFA tukee myös samanaikaisesti kolmannen osapuolen autentikointijärjestelmiä ja tarjoaa mahdolisuuden lisätä uusia helposti hallittavia ja käytettäviä autentikointifaktoreita, kuten RSA SecurID Tokens (laitteisto- ja ohjelmistoperusteinen), IBM TouchToken – TOTP (Timed One Time Use Password), henkilökohtaisen identiteetin verifiointipalvelu sekä yleist pääsykortit (CAC eli Common Access Card). z/OS kykenee myös tunnistamaan autentikointiprosessin ajan auditointifaktorit. IBM MFA lisäksi helpottaa uusien samassa järjestelmässä toimivien autentikointimenetelmien arviointia erilaisille käyttäjäryhmille. IBM MFA integroituu RACF ja IBM Security zSecure-ratkaisujen kanssa. Kaikki MFA:n konfiguraatiodata varastoidaan RACF-ratkaisun tietokantaan, jolloin datan varmuuskopitointi- ja palauttaminen on joustavaa. (IBM Security zSecure Suite, 2017)

3.10.5 IBM QRadar Advisor with Watson

Tietoturvauhkien määrä ja saatavilla oleva uhkadata ylittävät huomattavasti jopa taitavimpien tietoturva-asiantuntijoiden kapasiteetin. Watson for Cyber Security laajentaa tietoturva-analyytikon kyvykkyyksiä kehittyneiden uhkien tunnistamisessa ja ymmärtämisessä pureutuen rakenteettomaan dataan (blogit, WWW-sivut, tutkimuspaperit) ja korreloiden sitä paikallisten tietoturvahyökkäyksien kanssa. QRadar tulkitsee rakenteetonta dataa, joka on luotu välittämään informaatiota ihmiseltä ihmiselle ja korreloi sitä rakenteellisen datan kanssa paljastaen uutta relevanttia informaatiota tietoturvahyökkäyksistä. QRadar Advisor etsii pimennossa olevia datapisteitä, joita muut sovellukset tai palvelut eivät löydä ja siten kykenee tarkemmin tunnistamaan uhkia. Tavoitteena on muodostaa strategia tietoturvauhkien torjumiseksi. (IBM)

Tietoturva-analyytikot joutuvat kärsimään datan ylikuormituksesta ja usein he eivät kykene hallitsemaan valtavaa määrää päivittäisiä hälytyksiä. Tilanne johtaa helposti siihen, että organisaation toiminnassa ei voida huomioida tietoturvauhkia riittävällä tasolla. IBM QRadar Advisor with Watson hyödyntää (Kuvio 41) IBM Watsonin kognitiivisia kyvykkyyksiä (tekoälyä) ja QRadar Security Platformin tietoturva-analyysiin kehitettyä alustaa paljastamaan piilossa olevia uhkia ja automatisoimaan niiden tunnistusprosessia. Järjestelmä tutkii automaattisesti vaarallisia indikaattoreita, hyödyntää kognitiivisia kyvykkyyksiä tarjoten kriittisiä näkemyksiä ja lopuksi kiihdyttää tietoturvauhkiin suuntautuvaa reaktiosykliä. QRadar Advisor with Watson hyödyntää myös Watson for Cyber

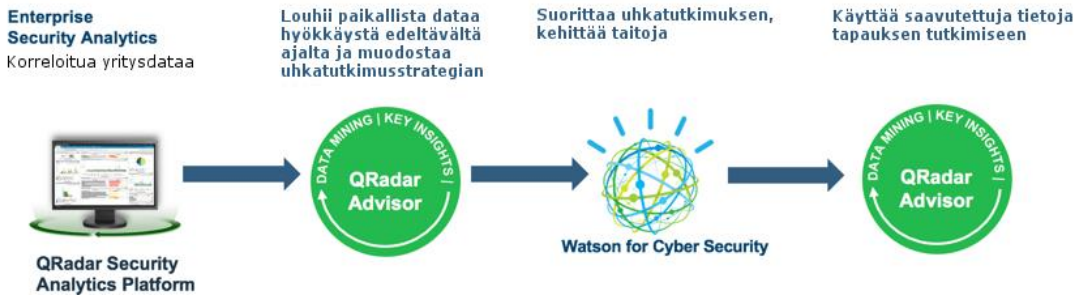
Securityn ominaisuuksia tietoturvauhkien tutkimisessa ja niihin vastaamisessa. (IBM QRadar Advisor with Watson)



Kuva 41 IBM QRadar Advisor with Watson-käyttöliittymä(Stasio, 2015)

QRadar Advisor with Watson toimii seuraavien vaiheiden (Kuvio 42) kautta:

1. QRadar Security Intelligence-alustan tunnistaessa tietoturvallisuusuhan, tietoturva-analyytikko voi siirtää sen QRadar Advisor with Watsonille tarkempaa tutkimusta varten. Advisor tekee ensin tietoturvauhkaa koskevan laajemman kartoituksen louhimalla lokaalista QRadar-ohjelmistosta saatavaa dataa. Tämän jälkeen ohjelmisto hyödyntää Watson for Cyber Security-ohjelmistoa tarkemman analyysin suorittamiseksi tietoturvauhasta.
2. Watson for Cyber Security tutkii tietokantaa, joka koostuu sadoista tuhansista lähteistä, jotka on kerätty esimerkiksi WWW-sivuilta, tietoturvafoorumeilta ja uutiskoosteista, ja koostaa näistä ymmärrettävän kokonaisuuden. Tämän jälkeen ohjelmisto etsii tietoturvauhkaan liittyvää lisäinformaatiota koskien haitallisia tiedostoja ja epäilyttäviä IP-osoitteita.
3. Lopuksi QRadar Advisor with Watson prosessoi informaatiota, jota se saa Watson for Cyber Security-ohjelmistolta etsien tietoturvauhkaan liittyviä avaintekijöitä.



Kuva 42 IBM QRadar Advisor with Watson toimintaperiaate (Dheap, 2017)

IBM QRadar with Watsonin avainominaisuuksia ovat automaattinen uhkatapausten tutkiminen, tekoälyn hyödyntäminen ja korkean tason riskien havaitseminen. QRadar toteuttaa paikallista tiedon louhintaa tietoturvahyökkäyksistä keräten aineistoa. Tämän jälkeen sovellus tarkastaa, onko jokin tai jotkin tietoturvauhista läpäisseet kerroksittaiset suojaukset vai ovatko ne estetty. Luetteloiden ja tiettyjen sopivien indikaattoreiden avulla tarkastusta voidaan automatisoida. Kognitiivisen päättelyn avulla voidaan tunnistaa todennäköisimmät uhat ja yhdistää uhkat alkuperäisiin tapahtumiin, kuten haitalliset tiedostot ja epäilyttävät IP-osoitteet yhteyksien piirtämiseksi näiden välille. QRadar lisäksi automaattisesti käyttää Watson for Cyber Securitya ulkoisen rakenteettoman datan, kuten WWW-sivujen, foorumien ja treat intelligencen hyödyntämiseksi. IBM QRadar myös paljastaa tapahtumien kriittisyyden, eli onko haittaohjelma suoritettu vai ei, mahdollistaen tehokkaaman ajankäytön korkeamma prioriteetin riskien tarkastelemiseen. (IBM QRadar Advisor with Watson)

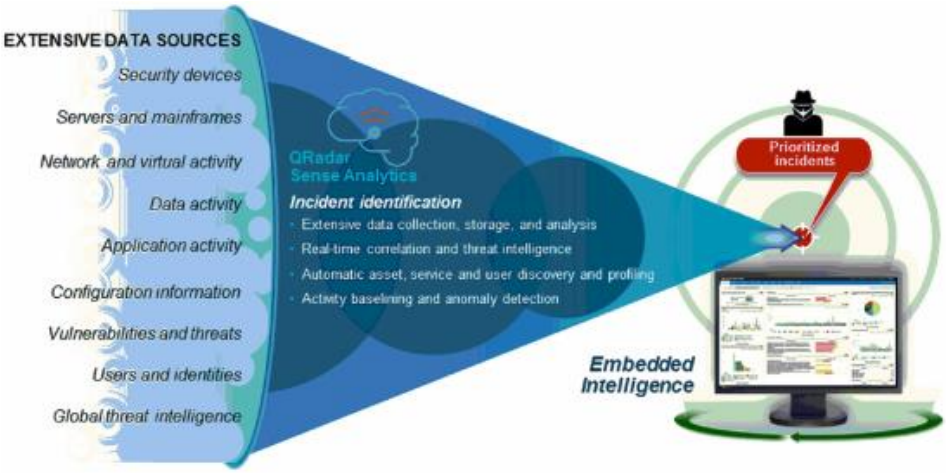
3.10.6 IBM QRadar Information Security and Event Mgmt (SIEM)

SIEM-ohjelmistot yhdistävät useita erilaisia tietoturvaohjelmistokomponentteja yhdeksi alustaksi. Yritykset hyödyntävät SIEM-ohjelmistoja keskittääkseen tietoturvaoperaatiot yhteen sijaintiin. Asiantuntijaryhmät, jotka hoitavat IT- ja tietoturvaoperaatioita, voivat päästä käsiksi samaan informaatioon ja hälytyksiin tehokkaamman kommunikaation ja suunnittelun mahdollistamiseksi. Tämänkaltaiset tuotteet tarjoavat kyvykkyyksiä, joiden avulla tietoturva-asiantuntijat voivat tunnistaa ja saada hälytyksiä IT-järjestelmissä havaituista anomalioista. Anomaliat voivat olla uusia haittaohjelmia, hyväksymättömiä järjestelmään kirjautumisia tai uusia havaittuja haavoittuvuuksia. Tietoturva-asiantuntijat tuottavat reaaliaikaista analyysiä IT-järjestelmien toiminnallisuuksista ja tietoturvasta sekä tallentavat lokitietoja ja muuta informaatiota raportointeja varten. Heillä on käytössään myös työkaluja, joiden avulla he voivat tunnistaa ja varmistaa, että ainoastaan riittävien käyttöoikeuksien haltijat voivat päästä käsiksi kriittisiin järjestelmiin. (G2 Growd, 2018)

IBM QRadar SIEM voi toimia tietoturvaratkaisuna pienelle, keskisuurelle tai suurelle organisaatiolle ja sen avulla voidaan kerätä, normalisoida ja korreloida tietoverkoissa liikkuvaa dataa hyödyntämällä vuosien aikana kertynyttä kokemusta. QRadar SIEM integroituu satoihin IBM:n ja muiden valmistajien tuotteisiin. Lisäksi QRadar tarjoaa kattavan

näkymän tietoturvatapahtumiin, jotka voivat liittyä organisaation tiloissa, hybridi- tai pilviympäristöissä tapahtuviin tapahtumiin. SIEM-ratkaisun keskiössä on kehittynyt analytiikkamoottori, joka on suunniteltu keräämään reaaliaikaista lokitietoa ja tietoverkon virusinformaatiota sekä hyödyntämällä kehittynyttä analytiikkaa mahdollisten hyökkääjien tunnistamiseksi. (IBM QRadar SIEM, 2014)

QRadar SIEM on skaalautuva ratkaisu, joka kerää ja hyödyntää tuhansien hajautettujen tietoverkon laitteiden lähettämää dataa tallentaen kaiken toiminnan ja tietoturvatapahtumat tietokantaan sekä hyödyntämällä analytiikkakyvykkyyksiä erottamaan oikeat uhat vääristä positiivisista (Kuvio 43). Lisäksi ratkaisu kaappaa TCP-IP-kerroksen 4 verkon virtausdataa ja kerroksen 7 sovelluksien hyötykuormia hyödyntämällä IP-pakettien tarkastusteknologiaa. QRadarin intuitiivinen käyttöliittymä auttaa IT-asiantuntijoita nopeasti tunnistamaan ja puuttumaan tietoverkkohyökkäyksiin oikealla prioriteetilla. Ratkaisu karsii satojen hälytyksien ja poikkeavien tapahtumien joukosta huomattavasti pienemmän ydinjoukon, jota voidaan tarkastella lähemmin. Nämä poikkeavat tapahtumat voivat sisältää sovelluksien sopimatonta käyttöä tai hyödyntämistä laittomiin tarkoituksiin, organisaation sisäisiä huijausyrityksiä ja varkauksia sekä uhkia, jotka useimmiten hukkuvat miljoonien tietoturvatapahtumien joukkoon. (IBM QRadar SIEM, 2014)



Kuva 43 IBM QRadar analysoi datalähteitä muokaten listan jatkotutkimuksia varten (IBM QRadar SIEM, 2014)

QRadar SIEM kerää erilaisista lähteistä informaatiota, kuten:

- **Tietoturvatapahtumat** (security events): Palomuureista, VPN-verkoista, tunkeutumisen havaitsemisen tunnistus- ja estojärjestelmistä, tietokannoista jne.
- **Tietoverkkotapahtumat** (network events): Kytkimistä, reitittimistä, palvelimista, isännistä jne.
- **Tietoverkon aktiviteettikonteksti** (network activity context): TCP/IP-kerroksen 7 sovelluskonteksti
- **Käyttäjäkonteksti** (user or asset context): Identiteetin ja pääsynhallintaa hoitavien tuotteiden sekä haavoittuvuuksia paljastavien skannereiden kontekstuaalinen data

- **Käyttöjärjestelmäinformaatio** (operating system information): Tuotteen myyjän nimi ja versionumero
- **Sovelluslokit** (application logs): ERP, työn kulku, sovelluksien tietokannat, hallinta-alustat jne.
- **Tietoturvauhkainformaatio** (threat intelligence): Erilaisista lähteistä, kuten IBM X-Force

QRadar SIEM jäljittää merkittäviä tietoturvatapahtumia ja uhkia tarjoten tietoturva-asiantuntijoille yksityiskohtaista informaatiota, kuten hyökkäyksen kohde, aika, haavoittuvuuden tila, hyökkäyksiä toteuttavien henkilöiden identiteetit, hyökkäysprofiilit, aktiivisena olevat uhat ja data aiemmista hyökkäyksistä jne. Edellä mainittu informaatio auttaa tietoturva-asiantuntijoita muodostamaan toimintastrategian ongelman ratkaisemiseksi. Reaaliajassa tapahtuva, paikkatietoa ja tapahtuman historiallista informaatiota hyödyntävä analysointi voi huomattavasti parantaa organisaation kykyä tutkia ja ratkaista erilaisia tietoturvatilanteita. (IBM QRadar SIEM, 2014)

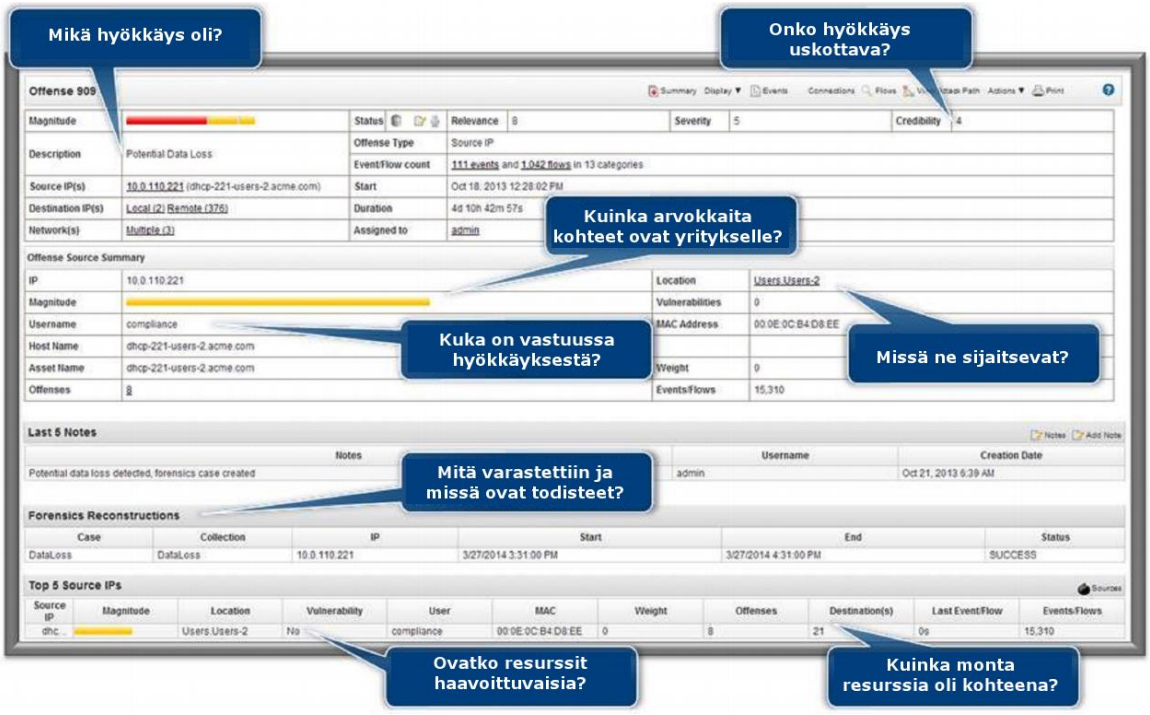
QRadar sisältää useita erilaisia anomalioiden tunnistuskyvykkyyksiä, jotka voivat olla indikaatioita organisaation sisäisistä uhista. QRadar SIEM kykenee tunnistamaan tilanteet, jossa sovelluksia tai pilvipalveluita käytetään huomattavasti tai ne eivät ole käytössä ollenkaan. Lisäksi QRadar osaa tunnistaa, mikäli tietoverkon aktiivisuustila eroaa huomattavasti historiallisesta tai keskimääräisestä aktiivisuudesta ja oppii tunnistamaan nämä päivittäiset tai viikoittaiset käyttöprofiilit. Tämä auttaa tietoturva-asiantuntijoita nopeasti tunnistamaan merkittäviä anomalioita. Lisäksi tietoturva-asiantuntijat voivat tehdä yhdistettyjä hakuja maantieteellisesti laajassa hajautetussa ympäristössä. (IBM QRadar SIEM, 2014)

QRadar SIEMin keskitetty tietokanta tallentaa tietoturvatapahtumien lokitietoja sekä tietoverkon verkkoliikenneinformaatiota yhteen paikkaan. Tällöin voidaan havaita, mikäli samasta IP-osoitteesta peräisin olevat erilliset tietoturvatapahtumat korreloivat kaksisuuntaisen tietoverkon liikennöintiaktiviteetin kanssa. QRadar SIEM kykenee myös ryhmittelemään verkkoliikennettä ja tallentamaan kapean aikaikkunan aikana tapahtuvia tietoturvatapahtumia yhdeksi tietokannan tietueeksi, joka osaltaan säästää tallennustilaa. (IBM QRadar SIEM, 2014)

QRadar SIEM kykenee monitoroimaan sovelluksien sekä järjestelmien, kuten ERP, tietokannat, Skype, VoIP (Voice Over IP eli IP-puhe) ja sosiaalinen media, dataa. Tämä sisältää informaation siitä, kuka käyttää ja mitä, analyysit sekä hälytykset koskien sisällön siirtoa ja korreloinnin muun tietoverkossa tapahtuvan aktiviteetin kanssa, jotta luvattomat tiedonsiirrot ja poikkeavat käyttäytymismallit paljastuisivat. Sen lisäksi, että QRadar SIEM sisältää jo useita erilaisia anomalioiden ja käyttäytymisen tunnistuksen säännöstöjä, tietoturva-ammattilaiset voivat luoda omia sääntöjään hyödyntäen suodattimia, jotka tarjoavat mahdollisuuden anomalioiden tunnistamiseksi aikasarajadatan varalta. (IBM QRadar SIEM, 2014)

IBM QRadar SIEM tarjoaa organisaation tietoturva-asiantuntijoille keskitetyn käyttöliittymän, joka mahdollistaa toiminnoittain jaotellun roolipohjaisen käytön ja reaaliaikaisen analyysinäkymän, tapahtumien hallinnan ja raportoinnin. QRadar SIEMissä on viisi oletusnäkyää, mukaan lukien tietoturva, tietoverkon aktiivisuus, sovellusten aktiivisuus, järjestelmän monitorointi ja sisäinen valvonta. Lisäksi käyttäjät voivat luoda ja räätälöidä omia työtilojaan. Tämänkaltaiset dashboard-kojelaudat helpottavat huippujen etsimistä hälytyksien joukosta, jotka voivat indikoida alkavaa hyökkäystä. Graafien avulla tietoturva-asiantuntijat voivat nopeasti tutkia korostuneena olevia tietoturvatapahtumia tai tietoverkossa virtaavaa liikennettä, jotka ovat epäilyksen kohteena. (IBM QRadar SIEM, 2014)

Kuviossa 44 kuvataan, miten QRadar SIEM tarjoaa informaatiota epäillyistä tietoturvahyökkäyksistä, miten arvokas kohde on liiketoiminnan kannalta, kuka on vastuussa hyökkäyksestä, missä hyökkääjä sijaitsee, mitä on varastettu ja missä ovat todisteet. Lisäksi näkymästä ilmenee viisi tärkeintä IP-osoitetta ja informaatiota siitä, ovatko jotkin kohteista haavoittuvaisia ja kuinka monta kohdetta on mukana jne.



Kuva 44 QRadar SIEM tarjoaa informaatiota hyökkäyksistä ja työkaluja säännöstöjen muokkaamiseen väärien positiivisten tulosten vähentämiseksi (IBM QRadar SIEM, 2014)

3.10.7 IBM QRadar User Behavior Analytics

Loppukäyttäjien käyttäytymisanalyysi (User Behavior Analytics eli UBA) on ollut jo viime aikoina paljon huomiota saanut keskustelunaihe tietoturvassa. Organisaation ulkoisia uhkia vastaan rakennettua suojausta kehitettäessä niiden on myös huolehdittava uhkista, jotka voivat aiheutua sisältäpäin. Uhkia voivat aiheuttaa muun muassa tahallista haittaa aiheuttava työntekijä, huolimaton liiketuttavuus tai ulkoinen toimija. Tämänkaltaiset uhat ovat vaikeita tunnistaa ja ne voivat aiheuttaa huomattavaa tuhoa yrityksen omaisuudelle heikentäen yrityksen aineetonta omaisuutta ja kuluttajien luottamusta sekä vahingoittaa organisaation brändiä ja mainetta. (Patel, 2017)

Esimerkiksi vuonna 2016 tapahtunut hyökkäys sähköverkkoa kohtaan Ukrainassa aiheutti sähkökatkoksen 200 000 asiakkaalle. Hyökkäys sai alkunsa työntekijän avatessa infektoituneen Word-dokumentin, jonka kautta hyökkääjät onnistuivat lähettämään haittaohjelman sähkölaitoksen työntekijöille ja näiden avulla kyeten varastamaan kriittistä informaatiota ja sulkemaan sähkölaitoksen järjestelmiä. Hyökkäys kulutti 200 megawattia kapasiteetista, joka oli 20 prosenttia Kiovan kaupungin yönaikaisesta kulutuksesta. Hyökkäys oli ensimmäinen suuri hyökkäystapahtuma kansakunnan sähkölaitosta vastaan, joka herätti paniikkireaktoita myös länsimaissa. (Condliffe, 2016)
Edellä mainitun kaltaisia hyökkäyksiä vastaan on kehitetty käyttäytymisanalyysiin perustuvia ratkaisuita, joista IBM QRadar UBA-sovellus on yksi suosituimmista alustoista IBM Security App Exchange-ekosysteemissä. IBM:n UBA-sovellusta on ladattu yli 4000 kertaa ja sitä on hyödynnetty loppukäyttäjien poikkeavien toimien tunnistamiseen. QRadar UBA-sovellus on tunnistanut muun muassa seuraavanlaisia käyttäytymismalleja (Patel, 2017):

- Järjestelmien ylläpitäjät ovat muuttaneet loppukäyttäjien attribuutteja ilman lupaa
- Käyttäjät ovat jakaneet VPN-verkon pääsytietoja
- Laitteita on viety pois maasta käyttäjien ollessa lomalla
- Käyttäjät esimerkiksi Pohjois-Amerikassa ovat lukeneet sähköpostiviestejä pilvipalvelussa ja muutamien minuuttien päästä tileille on koetettu kirjautua ulkomailta
- Tietoturvaoperaatioiden keskuksen (Security Operations Center eli SOC) asiantuntijoiden tilit ovat infektoituneet haittaohjelmien vuoksi
- Tietoturvatyökalujen havaitut väärinkäytökset
- Käyttäjät ovat avanneet henkilökohtaisia tilejä palvelimilla
- Enemmän kuin oletettu määrä sisäänkirjautumisia

Koneoppimisen algoritmeja voidaan hyödyntää loppukäyttäjän tavanomaisen käyttäytymisen ymmärtämisessä ja merkityksellisten poikkeamien havaitsemisessa. Koneoppimisen algoritmeja on sisällytetty IBM:n QRadar UBA-sovellukseen, jotta loppukäyttäjien epäilyttävä käytös ja poikkeava toiminta voidaan havaita. Nämä koneoppimisen algoritmit kykenevät tunnistamaan ajallisia ja aikasarjan poikkeavuuksia. Poikkeavuuksien tunnistamiseksi käyttäjien toimintaa monitoroidaan ja monitoroinnin perusteella luodaan normaalin käyttäytymisen, resurssien ja verkkoviestinnän hyödyntämisen toimintamallit. Näitä malleja voidaan hyödyntää haluttaessa määrittää, milloin loppukäyttäjä alkaa tehdä jotain uutta. Algoritmit kykenevät tunnistamaan ja ilmoittamaan poikkeavasta

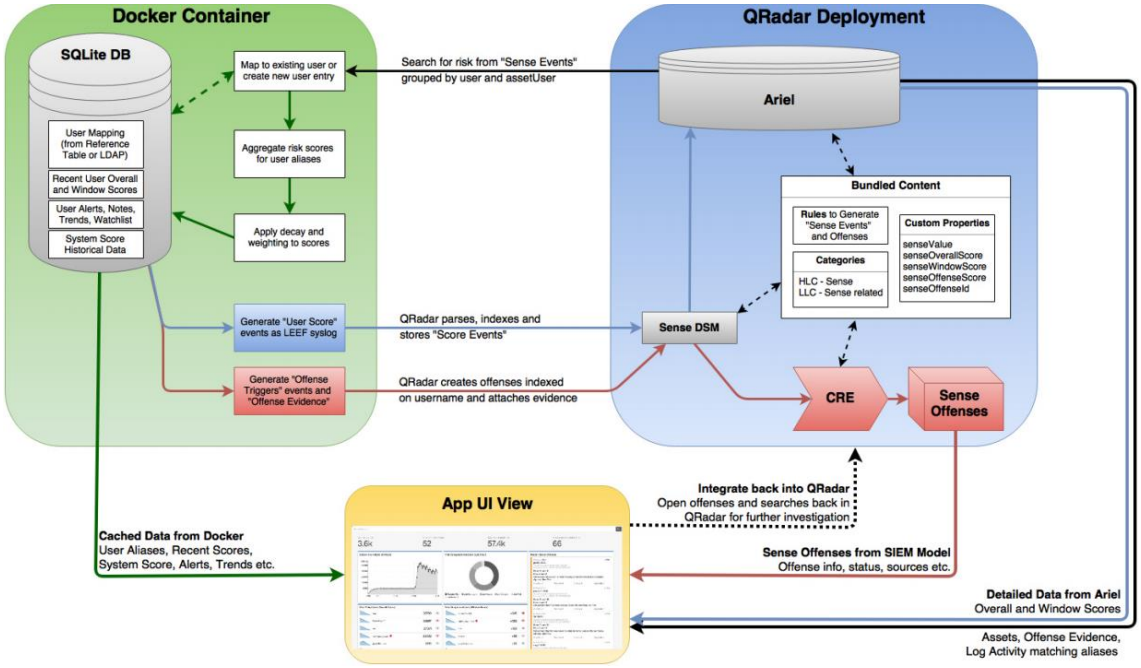
käyttäytymisestä sekä käynnistävät UBA-sovelluksen, jonka käyttäjien riskipisteitä nostetaan aina tarpeen vaatiessa. (Patel, 2017)

Monitoroimalla jokaisen organisaation tietojärjestelmän loppukäyttäjän aktiviteettia, työkalu kykenee tunnistamaan rooleja, joita käyttäjällä on organisaatiossa, jolloin käyttäjät voidaan jakaa roolipohjaisiin vertaisryhmiin. Uudenlainen käyttäytyminen, joka poikkeaa näistä rooleista, voidaan tunnistaa ja se voi olla alkuvaiheen indikaattori haitallisista tarkoitusperistä. Algoritmit toimivat itsenäisesti ja tarkkailevat käyttäjän aktiviteetteja useista eri näkökulmista, jotta väärien positiivisten tulosten määrä voi vähentyä. (Patel, 2017) Kyseiset algoritmit monitoroivat laajaa käyttötapausten aluetta, kuten:

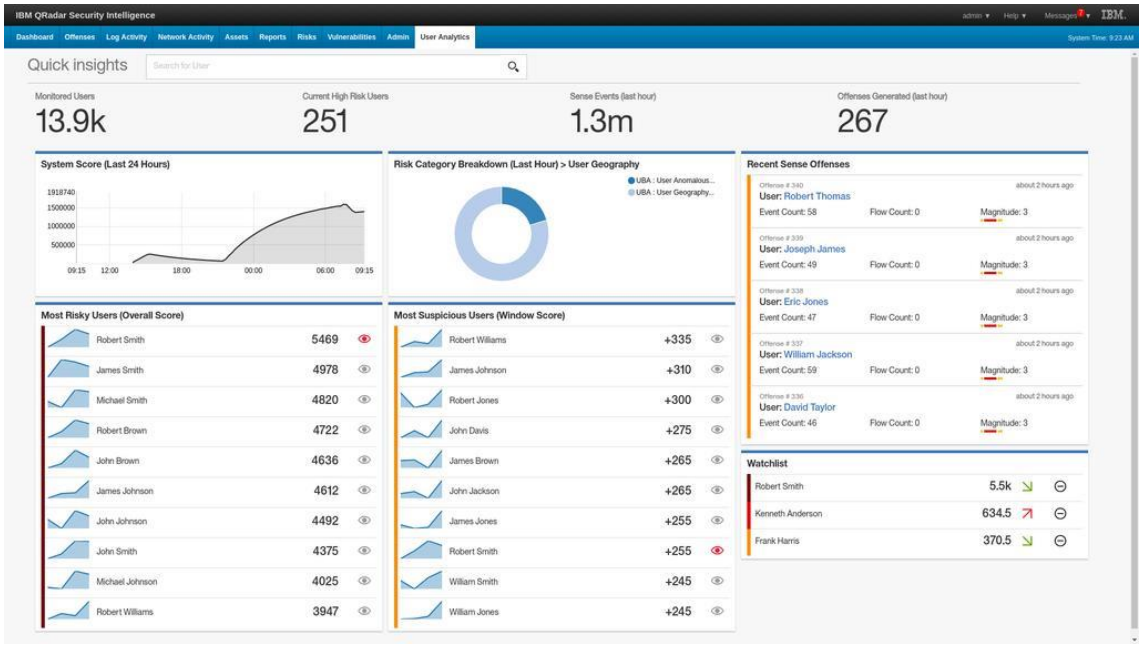
- Loppukäyttäjien aktiviteettien muutokset ilman muutosta niiden toistuvuudessa
- Muutokset aktiviteetin toistuvuudessa ilman aktiviteettiin kohdistuvia muutoksia
- Muutokset loppukäyttäjien aktiviteetin aikaikkunassa
- Datan suodattaminen laitteesta tai verkon kautta

Kuviossa 44 havainnollistuu UBA-sovellus ja sen integraatio QRadar-järjestelmän kanssa. UBA-sovellus toimii QRadar-järjestelmän kanssa keräten dataa organisaation verkossa olevista käyttäjistä. Kuviosta 44 ilmenee, että UBA-sovelluksen graafiseen käyttöliittymään kerätään tietoja Docker-säiliöstä (SQLite-tietokanta). Kerättäviä tietoja ovat muun muassa käyttäjien peitenimet, viimeiset riskipisteet (Kuvio 45), järjestelmän pisteet, hälytykset, trendit jne. Käyttöliittymään päivittyy informaatiota myös QRadar-järjestelmän puolelta. QRadar-järjestelmän toimittamaa informaatiota ovat hyökkäykseen liittyvä informaatio, tila ja lähteet. Lisäksi QRadar-järjestelmän ARIEL-tietokannasta saadaan muun muassa yleislaatuista dataa ja käyttäjien aktiviteetin kirjaustietoja, jotka vastaavat peitenimillä toteutettuja aktiviteetteja. UBA-sovellus lähettää QRadar-järjestelmälle informaatiota meneillään olevista hyökkäyksistä tarkempia tutkimuksia varten.

UBA-sovellukseen määriteltyjen säännöstöjen perusteella sovellus etsii asioita, joita loppukäyttäjät voivat tehdä ja jotka aiheuttavat ”sense event”-tapahtuman, jonka UBA-sovellus rekisteröi. Sovelluksen säännöstöt vaativat, että tapahtumilla on käyttäjätunnus ja lisäksi muita testejä. Seuraavaksi UBA lukee ”sense event”-tapahtumasta senseValue-arvon ja käyttäjätunnuksen sekä kasvattaa käyttäjän riskipisteitä senseValue-arvon verran. Käyttäjän riskipisteiden ylittäessä UBA-sovelluksen asetuksiin asetetun kynnysarvon, UBA-sovellus lähettää event-tapahtuman, joka laukaisee UBA-sovelluksen ”UBA: Create Offence”-säännön ja siten sääntörikkomus on luotu kyseiselle käyttäjälle.



Kuva 44 IBM QRadar User Behavior Analytics-prosessikaavio (IBM User Guide, 2018)

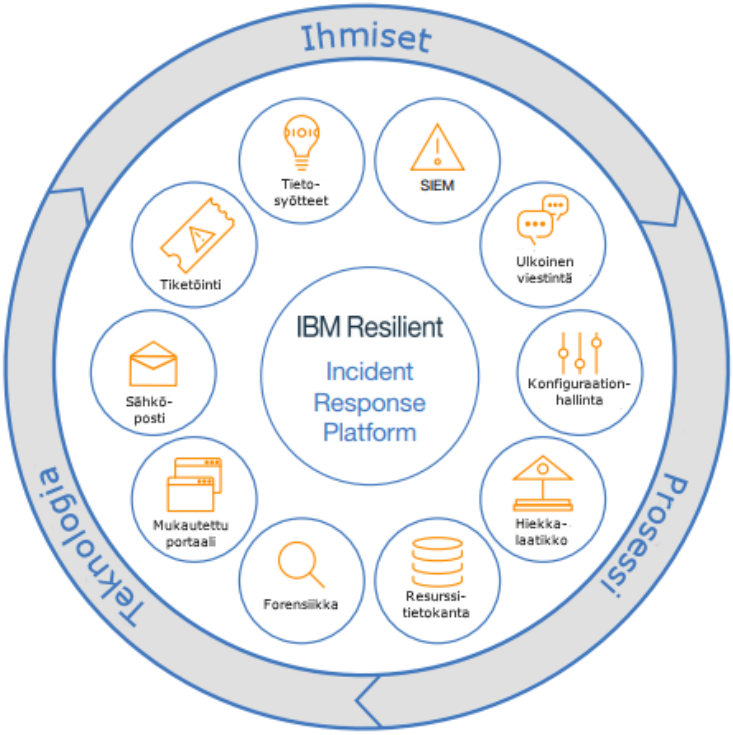


Kuva 45 IBM QRadar User Behavior Analytics dashboard-kojelautanäkymä (IBM Security, 2016)

3.10.8 IBM Resilient Incident Response Platform (IRP)

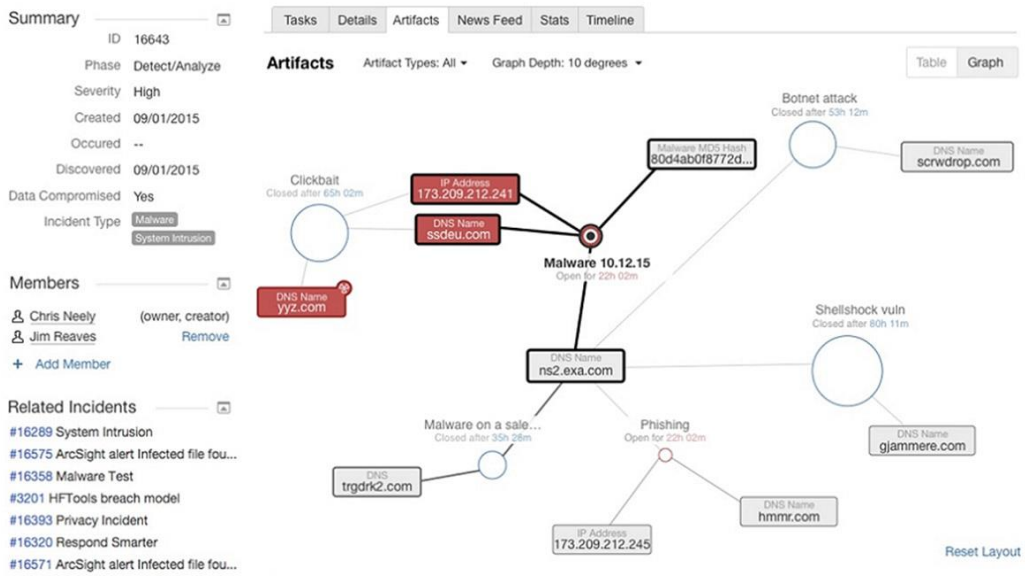
IBM Resilient Incident Response Platform (IRP) on yksi johtavista alustoista tapahtumaprosessien automatisoimiseksi. IRP integroituu organisaation jo olemassa oleviin tietoturva- ja IT-investointeihin ja se tarjoaa keskitetyn alustan kyberhyökkäysten tutkintaan ja niiden estämiseen. IRP antaa tietoturva-asiantuntijoille mahdollisuuden analysoida, vastata ja lieventää tietoturvatapauksia nopeammin, älykkäämmin ja tehokkaammin. IRP tarjoaa arvokasta informaatiota meneillään olevista tietoturvallisuuteen liittyvistä tapahtumista antaen tietoturvaan erikoistuneille asiantuntijoille mahdollisuuden eliminoida tai tehostaa kriittisiä askelia. IRP soveltuu useille eri kokoisille ja rakenteisille organisaatioille soveltuen erityisen hyvin niin suurten kuin keskisuurten yritysten käyttämille monimuotoisille järjestelmille aina pieniin IT-tietoturvatiimeihin saakka. (IBM Resilient)

IBM Resilient Incident Response-alusta jakaantuu kolmeen osa-alueeseen (Kuvio 46), jotka ovat ihmiset, teknologia ja prosessit. Ihmiset-osa-alueeseen kuuluu organisaatioiden välinen koordinaatio HR-osaston, IT-osastojen, johdon ja turvallisuusoperaatioiden keskuksen (SOC eli Security Operations Center) välillä. Teknologian osa-alue käsittää IBM Resilient Incident Response-alustan tarjoaman avoimen alustan, joka integroituu organisaation tietoturvainfrastruktuuriin muodostaen keskuksen tietoturvatapahtumien käsittelemiseksi. Prosessit osa-alue tarjoaa dynaamisen ohjeistuksen organisaation jäsenille, jotta he ymmärtävät roolinsa ja vastuunsa kyberturvallisuuden suhteen tietoturvatapahtumaa (kuten hyökkäys) ennen, sen aikana ja hyökkäyksen jälkeen.



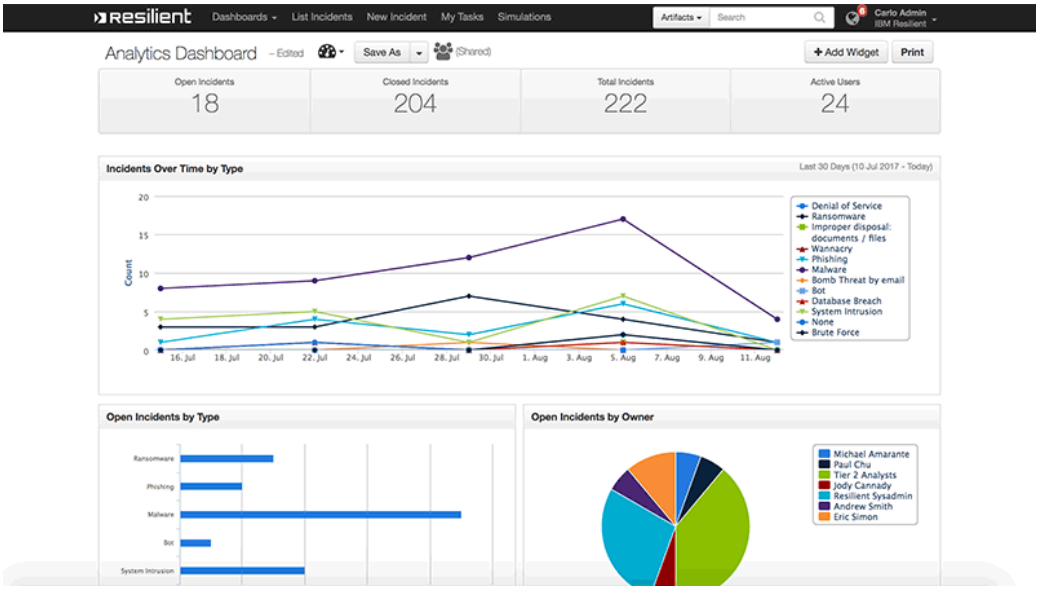
Kuva 46 IBM Resilient Incident Response Platform-palvelut
(Managed Security Services Orchestration, 2017)

Kuviossa 47 esitelty Resilient Incident Visualization havainnollistaa graafisesti tietoturvatapahtuma-artifaktien ja organisaation sisällä tapahtuvien tietoturvatapahtumien, niin sanottujen murtoskannereiden (IoC eli Indicator of Compromise) keskinäiset suhteet. Kyberturvallisuudessa artifaktit voivat tarkoittaa dataa, joka ei ole tutkimuksen tai vasteen kannalta relevanttia. Esimerkiksi käyttöjärjestelmien rekisteriavaimet, aikaleimat tai lokitiedot voivat olla sellaisia. Graafinen visualisaatio tarjoaa tietoturva-ammattilaisille keinon nähdä moniulotteisena olennaiset artifaktien ja tietoturvatapausten väliset suhteet, jolloin he voivat tarkastella hyökkäyksen historiatietoja eli miten hyökkäys on kehittynyt ajan funktiona. Tämä mahdollistaa nopean vasteen, jolloin tietoturva-asiantuntijat voivat tutkia hyökkäystä tai tehdä korjaavia toimenpiteitä suoraan visualisesta näkymästä. (Bruce, 2016)



Kuva 47 IRP-alustan tietoturvatapahtumien visualisointi
(IBM Resilient Incident Response Platform, 2017)

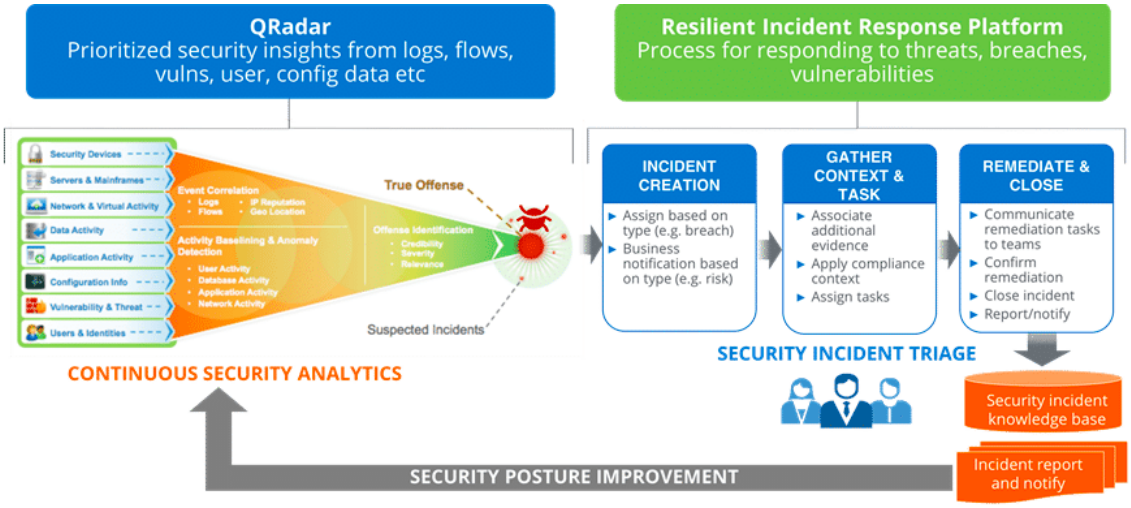
Kuviosta 48 havainnollistuu IBM Resilient Incident Response-alustan dashboard-kojelautanäkymä, jossa on esitettynä organisaation tietoturvatapausten avaininformaatio. Kojelautanäkymästä voidaan havaita avoimet ja suljetut tietoturvatapahtumat, kaikki tapahtumat yhteensä ja aktiiviset käyttäjät. Kojelautanäkymän graafit havainnollistavat ajan funktiona esiintyviä tietoturvatapahtumia, kuten DoS-hyökkäykset, kiristysohjelmat (ransomware), kalasteluhyökkäykset (phishing), haittaohjelmat (malware), botit (Bots), brute force-hyökkäykset, tietokantamurrot (data base breach) tietojärjestelmiin tunkeutumiset (system intrusion), sähköpostin kautta tapahtuva pommitus (bomb threat by email) jne. Kojelautanäkymästä ilmenee myös tyypeittäin ja asiakkuuksittain (henkilöittäin) luokitellut avoimet tietoturvatapaukset.



Kuva 48 IRP-alustan raportointi ja kojelaudat (IBM Resilient Incident Response Platform, 2017)

Haittaohjelmahyökkäyksen (Malware) ja QRadar-ohjelmiston säännöstön perusteella tapahtuma generoidaan automaattisesti Resilient-alustassa, johon sisällytetään relevanttia informaatiota hyökkäyksestä ja vaarantavista indikaattoreista. Seuraavaksi Resilient-alusta generoi yksityiskohtaisen toimintasuunnitelman koettua uhkaa varten sekä lisää mukaan siihen liittyviä indikaattoreita, kuten haittaohjelmatarkisteen (HASH). Haittaohjelmaa verrataan IBM X-Force Exchangen tuottamiin syötteisiin, joiden perusteella voidaan varmistaa, että haittaohjelma on luotettavasti tunnistettu haitalliseksi. Lisäksi voidaan tarkastella esimerkiksi kalasteluhyökkäyksien (phishing attacks) ja niihin liittyviä IP-osoitteita. Saatua yksityiskohtaista informaatiota voidaan sitten hyödyntää ongelman korjaamiseksi, kuten esimerkiksi firmware-päivitysten mahdollisesti mukanaan tuomien hyökkäysten estämisessä.

Kuviossa 49 on havainnollistettu QRaradar- ja Resilient Incident Response alustan integraatiota, jonka malli on hyödynnettävissä minkä tahansa SIEM (Security Information and Event Management) -ratkaisun kanssa. SIEM-ratkaisu tarkkailee organisaation tietojärjestelmiä- ja verkkoja sekä hälyttää havaitessaan normaalista poikkeavaa toimintaa. Mikäli tietoturvauhat havaitaan aikaisessa vaiheessa, nopea reagointi niihin mahdollistuu vahingot minimoiden. SIEM-ratkaisun taustalla on ajatus, että tekniset ratkaisut, kuten palomuurit ja IDS/IPS-tuotteet eivät aukottomasti kykene torjumaan kaikkia uhkia, joita ammattimaiset tahot pyrkivät hyödyntämään myös pitkän ajan kuluessa. Ulkoisten uhkien lisäksi myös organisaatioiden sisäiset tietoturvauhat ja tietovarkaudet saattavat olla ulkoisia hyökkäyksiä vaikeammin torjuttavia. SIEM:n tarkoitus on auttaa havaitsemaan suojausratkaisut läpäisevät hyökkäykset ja reagoimaan niihin mahdollisimman nopeasti. (Kinnunen, 2017) Organisaation jo olemassa olevaan SIEM-ratkaisuun yhdistetty QRadar- ja Relisient Incident Response Platform-ratkaisut tehostavat organisaation jo hyödyntävää SIEM-ratkaisun toimivuutta tarjoten työkaluja haittaohjelmien tunnistamiseen ja tietoturvauhkiin reagoimiseen.



Kuva 49 IBM Resilient Incident Response Platform ja QRadar integraatio(Northdoor, 2018)

3.10.9 IBM Security AppScan

Useimmat organisaatiot ovat riippuvaisia ohjelmistosovelluksista, jotka auttavat niitä harjoittamaan liiketoimintaprosessejaan, toteuttamaan transaktioita tavarantoimittajien kanssa ja toimittamaan palveluita asiakkaille. Usein tietoturva on kuitenkin ainakin osin unohtunut ja organisaatiot ovat voineet käyttää liian vähän resursseja tai laiminlyöneet tietoturvan kokonaan. Sovellukset voivat vaarantaa koko organisaation tietoturvan haavoittuvuuksiensa kautta, jolloin hyökkääjä kykenee hyödyntämään tietoturva-aukkoja ja pääsemään sisään organisaation tietojärjestelmiin ja niissä sijaitsevaan luottamukselliseen informaatioon ja asiakasdataan. (IBM Security Appscan Enterprise)

Vuosittain löytyy lähes 4000 uutta WEB-sovelluksien haavoittuvuutta ja 92 prosenttia kaikista tapauksista, joissa on ollut kyseessä datan häviäminen, johtuu juuri WEB-sovelluksiin kohdistuneista hyökkäyksistä. Reagoiva tietoturvahyökkäyksiä kohtaan kohdistuva lähestymistapa ei ole ollut riittävä keino pysyä yhä kehittyvien tietoturvahyökkäyksien mukana. Nykypäivän organisaatioiden tulee toteuttaa myös sovelluksiin kohdistuvia tietoturvaohjelmia ja vaatia ratkaisuja, jotka auttavat integroimaan tietoturvatestauksen osaksi ohjelmistokehityksen elinkaarta, jolloin haavoittuvuudet voidaan tunnistaa ja korjata, ennen kuin ne aiheuttavat uusia uhkia organisaatiolle. (IBM Security Appscan Enterprise)

IBM Security Appscan-sovellus tarjoaa kehittyneen sovellusten tietoturvan testauksen ja riskien hallinnan. IBM Appscan auttaa organisaatioita vähentämään organisaation hyödyntämien sovelluksien organisaatioon kohdistuvia riskejä hyödyntäen tietoturvatestausta, jonka avulla voidaan tunnistaa ja eliminoida haavoittuvuudet. Appscan auttaa myös kontrolloimaan sovellusprojektin kustannuksia tunnistamalla haavoittuvuuksia ja virheitä jo aikaisessa prosessin vaiheessa. Appscan kykenee myös monitoroimaan sovellusten tietoturvaohjelmien edistymistä ja hallinnoimaan sääntelyvaatimuksia, jotka on kehitetty suojaamaan WEB-sovellusten prosessoimaa sensitiivistä dataa. (IBM Security Appscan Enterprise)

Ohjelmistokehitystiimien ajaessa esituotantovaiheen testejä ennen sovelluksen julkaisemista, voi sovelluksen tietoturvasta tulla pullonkaula ohjelmistokehitysprosessissa. Ongelma on laaja, sillä organisaatiot kehittävät ja ajavat satoja tai tuhansia sovelluksia, jotka käsittelevät kriittisiä prosesseja ja dataa. Pieni tietoturva-asioihin keskittyvä ryhmä asiantuntijoita ei kykene hallitsemaan näin suurta kokonaisuutta ja heillä on käytännössä mahdollisuus testata vain pientä osaa sovelluksista. Tällöin organisaatio joutuu kohtaamaan yhä kasvavan riskin. Kriittisiä haavoittuvuuksia voidaan hyödyntää avaamaan tietoturva-aukkoja mahdollisille hyökkäyksille ja niistä aiheutuville mahdollisille datan häviämisille. (IBM Security Appscan Enterprise)

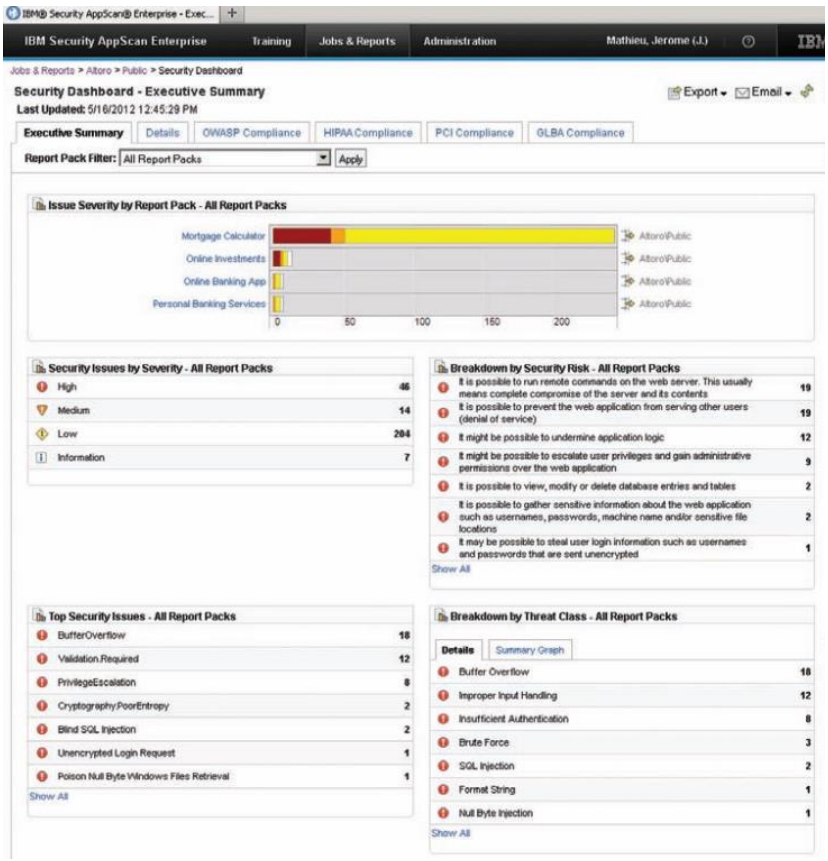
IBM Security Appscan tarjoaa kontrolloitua skaalautuvuutta, jotta koko ohjelmistokehityksen elinkaaren aikana tapahtuva sovellusten tietoturvatestaus mahdollistuu. Sen sijaan, että tietoturvatestejä suoritetaan vain kouralliselle sovelluksia, tietoturva-asiantuntijat voivat kirjoittaa testiscriptejä, joita voidaan hyödyntää osana ohjelmistokehityksen rutiineita ja laaduntarkastusprosesseja. Appscan-ohjelmistoa käyttävät tietoturva-analyytikot voivat määrittää tietoturvatestien käytänteitä ja sovelluskehittäjät voivat toteuttaa sovellusten tietoturvatestausta jo käännetyille sovelluksille käyttämällä Quick Scan Web-käyttöliittymää. Sovelluskehittäjät suorittavat staattista sovellusten lähdekoodin tietoturvatestausta integroidussa kehitysympäristössä tai sisällyttävät automaattisen tietoturvatestaamisen sovelluskehitysprosessiin. Tietoturvavaatimusten täyttämiseksi ohjelmistotestaajat ajavat dynaamisia tietoturvatestejä testitapauksineen, joita on määriteltyinä IBM Rational Quality Manager-ohjelmistossa. (IBM Security Appscan Enterprise)

Haavoittuvuuksien ja potentiaalisten riskitekijöiden tunnistamiseksi organisaatioiden tulee hyödyntää eri tietoturva-alan ammattilaisten yhteistyötä, kuten ohjelmistokehitykseen erikoistuneet ryhmät, ohjelmistotestaajat ja tietoturva-analyytikot. Appscan mahdollistaa yhteistyön koordinoinnin ja tarjoaa työkaluja yhteistyöhön edellä mainittujen tahojen välille. Työkalujen avulla haavoittuvuuksia voidaan priorisoida ja tapauksia voidaan avata riskien mukaisesti, testata ja vertailla testien tuloksia. Jokaista raportoitua haavoittuvuutta kohti IBM Security AppScan tarjoaa teknisen selityksen tapauksesta ja tietoturvariskin, jonka se nostaa esiin. Lisäksi AppScan ehdottaa ohjelmakoodiin liittyviä muutoksia, jotka voivat eliminoida haavoittuvuuden esiintymisen. Web-käyttöliittymän tai integroidun kehitysympäristön avulla ohjelmistokehittäjät voivat käsitellä tarvitsemaansa informaatiota ymmärtääkseen haavoittuvuuksia ja ryhtyäkseen toimiin ongelman korjaamiseksi. (IBM Security Appscan Enterprise)

IBM Security AppScan ja sen tarjoama keskitetty alusta mahdollistavat ohjelmistokehityksessä ja tuotannossa olevien sovellusten tietoturvatarkastuksien yhtäaikaisen suorittamisen. AppScan auttaa tietoturva-asiantuntijoita varmistamaan, että kaikki ohjelmistokehityksessä olleet sovellukset tarkastetaan ennen julkaisua ja kaikki tuotannossa olevat sovellukset voidaan säännöllisesti tarkastaa tietoturvauhkien ja haavoittuvuuksien varalta. Tämä ei kuitenkaan vielä riitä, vaan organisaation on tunnistamisen lisäksi myös toimittava aktiivisesti niiden uhkien poistamiseksi ja haavoittuvuuksien korjaamiseksi.

Tämä usein vaatii tietoturva-, ohjelmistokehitys- ja testausryhmien toimivaa yhteistyötä ja toimivaa alustaa tähän tarkoitukseen. (IBM Security Appscan Enterprise)

AppScan kykenee tarjoamaan alustan sovellusriskien hallintaan, johon kuuluu sovellusten ja prosessien havainnollistaminen kojelautanäkymässä (Kuvio 50), trendianalyysit (historia) ja KPI-indikaattorit avoimien tapausten monitoroimiseksi, korjaussyklit ja nykyinen sovelluksen riskitila. AppScanin ominaisuuksia ovat myös keskitetty hallinta, joka kattaa kaikki ohjelmistotuotannossa olevat sovellukset ja niiden säännölliset tietoturvatarkastukset ja vaatimustenmukainen raportointi, jota varten AppScan:ssa on 40 valmista mallia, joiden avulla sovelluksen tietoturva voidaan saattaa vastaamaan säännöksissä määriteltyjä malleja, kuten PCI, HIPAA ja EU Data Protecting Directive, Security Control Standard (ISO 27001) jne. (IBM Security Appscan Enterprise)



Kuva 50 IBM Security AppScan sovellusriskinäkymä(IBM Security AppScan Enterprise)

IBM AppScan yhdistää yhdessä ratkaisussa dynaamisen ja staattisen toiminnan ja tarjoaa hybridianalyysiominaisuuden, jossa integroidaan dynaaminen ja staattinen testaaminen yksityiskohtaisen analyysin sekä tarkkojen tuloksien aikaansaamiseksi. AppScan tarjoaa myös modulaarisen rakenteen, jonka avulla organisaatiot voivat räätälöidä tietoturvaratkaisunsa omien tarpeidensa mukaisesti. IBM Security AppScan-palvelin sisältää keskitetyn säiliön kaikkia sovellusten tietoturva-arviointeja varten. Lisäksi organisaatiot voivat suorittaa dynaamisia sovellusten tietoturvatestauksia IBM Security AppScan Enterprise Dynamic Analysis Scanneria hyödyntäen. Enterprise Dynamic Analysis Scanner-ohjelmistoa voidaan käyttää suorittamaan useita yhtäaikaisia dynaamisen analyysin arviointeja ja tarjoamaan organisaatioille skaalautuvan testiratkaisun heidän vielä ohjelmistokehitysvaiheessa, laatutestauksessa ja esituontanto- tai tuotantotestivaiheessa olevien sovelluksiensa haavoittuvuuksien testaamiseksi. IBM Security AppScan Source kykenee toteuttamaan staattisen koodin analyyseja tietoturvanäkökulmasta, jota tietoturva-asiantuntijat voivat hyödyntää asiakasohjelmiston kautta. AppsScan Sourcea voivat tietoturva-asiantuntijat hyödyntää myös sovelluskehitysympäristön kautta. Kaikki dynaamiset ja staattiset testitulokset yhdistetään IBM Security AppScan Enterprise-palvelimelle, joka tarjoaa keskitetyn alustan tietoturvatestaukseen ja sovellusten riskien hallintaan. Tuloksiin perustuen palvelin voi korreloida tuloksia hyödyntäen dynaamisia ja staattisia arviointeja, joiden perusteella voidaan tuottaa lisäinformaatiota löydetyistä haavoittuvuuksista ja ehdotuksia niiden korjaamiseksi. (IBM Security Appscan Enterprise)

IBM Security AppScan integroituu IBM QRadar Security Information and Event Management (SIEM)-ohjelmistoon, joka kerää, varastoi ja analysoi informaatiota sekä tarjoaa reaaliaikaisen tapahtumien korreloinnin tietoturvauhkien tunnistamiseen, säännösten mukaiseen raportointiin ja audintointiin. QRadar-integraatio helpottaa AppScanin tuottaman sovelluksien haavoittuvuuksista ja tietoturvauhkista kerätyn datan analysointia, jolloin QRadar seuloo ja poimii oleelliset ja varteenotettavat tietoturvauhkat, jotka uhkaavat juuri tietyn organisaation liiketoimintaa ja joihin tulee pikimmiten puuttua. Lisäksi sovelluksien haavoittuvuusdata tuodaan QRadar Risk Manager analytiikkamoottorille, jotta tietoturva-ammattilaiset voivat simuloida hyökkäyksiä ja määrittää haavoittuvuuksien ja uhkien aiheuttamat aukot puolustuksessa, jolloin niiden aiheuttama riski organisaatiolle voidaan määrittää. (IBM Security Appscan Enterprise)

3.10.10 IBM Security Guardum

IBM Security Guardum auttaa organisaatiota omaksumaan kokonaisvaltaisen tietoturvan toteuttamisen sekä analysoimaan ja suojautumaan ulkoisilta uhkilta. Nykyään tietoturvauhat ovat yleisempiä kuin aiemmin ja vaikuttavat yhä enemmän organisaatioiden toimintaan. Maailmanlaajuisten tutkimusten mukaan keskimääräinen tietoturvauhkista aiheutuva kustannus on nykyään 4 miljoonaa Yhdysvaltain dollaria. Kauppasalaisuuksien, tuotesuunnitelmien tai muiden IPR-oikeuden alaisten asioiden menettäminen voi johtaa organisaation taloudellisiin ongelmiin. Ydinliiketoimintoja koskeva kriittinen ja sensitiivinen data toimivat houkuttimena kyberhyökkäyksille ja toimivat niiden aktivoijina. (IBM Security Guardum, 2017, 1)

Perinteisesti organisaatiot ovat keskittyneet organisaation sisäisiin suojauksiin kriittisen informaation suojaamiseksi. Perinteiset työkalut, kuten virustorjuntaohjelmistot ja palomuurit eivät ole riittävä suoja uudenlaisia ja kehittyneitä uhkia vastaan, jotka usein tulevat organisaation sisältä. Lisäksi datan määrä kasvaa, muuttuu ja muovautuu jatkuvasti, jolloin suojautumistoimenpiteiden tulee seurata mukana. Yhä kasvava määrä käyttäjiä, sovelluksia ja järjestelmiä tarvitsevat välittömän pääsyn erilaiseen sensitiiviseen dataan, joka on tyypillisesti tallennettuna tietokantoihin, tietovarastoihin, erilaisille tiedostojen jakamiseen tarkoitetuille palvelimille, Big Data-alustoille, pilvipalvelualustoille jne. Oleellista on olla tietoisia siitä, keillä on oikeus käsitellä tämän kaltaista dynaamista ja hajautettua dataa ja kuka jakaa sitä ja kenelle. (IBM Security Guardum, 2017, 1)

IBM Security Guardum-alusta (Kuvio 51) on suunniteltu suojaamaan kriittistä dataa, missä tahansa se sijaitseekin. Alusta auttaa tietoturvaryhmiä automaattisesti analysoimaan, mitä tietojärjestelmän ympäristössä tapahtuu. Tällöin on mahdollista minimoida riskejä, suojella sensitiivistä dataa sisäisiltä ja ulkoisilta uhkilta, ja lisäksi omaksua muutoksia, jotka vaikuttavat tietoturvaan ja valvontaan. Hyödyntämällä alustan graafista käyttöliittymää, organisaation tietoturvaan erikoistuneet asiantuntijat voivat tunnistaa ja korjata sensitiiviseen dataan kohdistuvia riskejä. Alusta kykenee käsittelemään rakenteetonta ja rakenteellista dataa sekä relaatiotietokantoja, tietovarastoja, Hadoop-palvelua, NoSQL-tietokantoja jne. Monikerroksinen alustaratkaisu mahdollistaa automatisoidun tietoturvauhka-analyysien tekemisen, dynaamisen datan suojauksen ja koko organisaation laajuisen kattavuuden. (IBM Security Guardum, 2017, 2)

Guardum-alustan avulla tietoturva-asiantuntijat voivat:

- Etsiä ja luokitella sensitiivistä dataa ja oikeuksia sekä paljastaa riskejä automaattisesti.
- Tietää, kuka käsittelee dataa, huomata poikkeavuuksia (anomaliat) ja pysäyttää datan hävikki.
- Analysoida datan käytön malleja riskien selvittämiseksi ja korjaamiseksi.
- Tukea analysointia hyödyntämällä kehittyneitä analytiikan ja koneoppimisen menetelmiä, jotta epätavallinen käyttäytyminen ja riskikäyttäytyminen voidaan lopettaa.
- Hyödyntää uhkien tunnistusanalytiikkaa huomaamaan ja pysäyttämään tietomurrot ajoissa.
- Käyttää kojelauta (engl. dashboard) –näkymää esittäessään osakkeenomistajille tietoturvan tilan ja edistymisen ajan funktiona, jotta he voisivat saada paremman käsityksen siitä, minkälainen vaikutus Guardum-alustan hyödyntämisellä ja tietoturvalla on liiketoiminnassa.

Kuva 51 IBM Security Guardum toimintaperiaate (IBM Security Guardum, 2017, 2)

Guardum-alusta auttaa tietoturva-asiantuntijoita automaattisesti etsimään ja luokittelemaan sensitiivistä informaatiota graafista käyttöliittymää hyödyntäen. Alustan avulla tietoturvahenkilöstö voi löytää kaikki datan lähteet, jotka voivat sisältää sensitiivistä informaatiota, kuten luetteloimattomat tietokannat. Lisäksi tietoturvahenkilöstö voi hyödyntää räätälöitäviä luokittimia ja oikeuksien hallinnan kyvykkyyksiä automatisoidakseen tietoturvapolitiikan täytäntöönpanoa. Sensitiivisen datan etsiminen voidaan myös automatisoida säännölliseksi, jotta huijauspalvelinten käyttöönotto voidaan estää ja jotta voidaan varmistaa, ettei kriittistä informaatiota menetetä. (IBM Security Guardum, 2017, 2)

Sensitiivisen datan suojaamiseksi Guardum kykenee jatkuvasti monitoroimaan, kuka käyttää tai yrittää käyttää sensitiivistä dataa reaaliajassa. Guardum-alustassa on poikkeavuuksien tunnistuskyvykkyys, johon on sisäänrakennettu älykkyyttä riskien analysointia ja ymmärtämistä varten, mikä perustuu käytöksen muutoksiin. Alusta hyödyntää kehittynyttä koneoppimisen algoritmia, joka kykenee tunnistamaan epänormaalin datan käytön hyödyntäen yksityiskohtaista kontekstuaalista informaatiota. Adaptiivisen oppimisprosessin avulla alusta vertaa uusia normaaleja toimintamalleja uusiin toimintoihin niiden ilmetessä. Alustan intuitiivinen ja kognitiivinen käyttöliittymä auttaa paikantamaan poikkeavuuksia, jolloin ylläpitäjien on mahdollista pureutua ongelmaan ja etsiä sen aiheuttanut syy. (IBM Security Guardum, 2017, 3)

Guardum-alusta tarjoaa tietoturva-asiantuntijoille myös työkaluja, joiden avulla he voivat turvata liiketoimintaa taloudellisilta riskeiltä hyödyntäen kattavia audintointikyvykkyyksiä ja datan sisäistä valvontaa. He voivat myös suojata kriittistä dataa hyödyntämällä salauksia, naamiointeja (engl. masking), dynaamista estämistä, hälytyksiä ja karanteeneja jne. Lisäksi he voivat hyödyntää reaaliaikaista aktiviteetin monitorointia ja estämistä, jotta laiton sisäiseen tai ulkoiseen dataan kohdistunut käyttö voidaan estää.

Alusta kykenee estämään hyökkääjien pääsyn useimmissa erilaisissa lähteissä sijaitsevaan sensitiiviseen dataan, kuten pilvipalveluympäristöt, Big-data-alustat ja tiedostojärjestelmät. Alusta monitoroi tiedostojärjestelmiä reaaliajassa ja tarjoaa organisaatioille mahdollisuuden tunnistaa poikkeama, tallentaa se lokitietoihin ja estää luvattoman sensitiivisten resurssien käytön. Lisäksi alusta kykenee tunnistamaan organisaation jo hyväksyttyjen käyttäjien epäilyttävän toiminnan esimerkiksi tunnistamalla sensitiivisten tiedostojen ja hakemistojen massakopioinnin, tunnistamaan yksittäiset huiput tiedostojen hyödyntämisessä, generoimaan hälytyksiä sopimattomista tai luvattomista resurssien käytöistä, estää kaikkein sensitiivisimpien dokumenttien käytön ja generoimaan räätälöityjä raportteja kaikesta toiminnasta. (IBM Security Guardum, 2017, 4)

IBM Guardum-alusta tukee heterogeenista integraatiota muiden tietoturvateollisuuden johtavien tietoturvaratkaisujen, standardien ja sovellusten kanssa. Lisäksi se integroituu muihin IBM Security-tietoturvaratkaisuihin, kuten IBM QRadar, jolloin Guardum lähettää informaatiota tapahtumista ja tietokannoista. Guardum voi myös ottaa vastaan tila- ja hälytysilmoituksia QRadarilta, joka auttaa puolustautumaan IP-osoitehuijauksia, hyökkääjiä ja uudenlaisia haavoittuvuuksia vastaan. Guardum- ja QRadar-integrointi voi auttaa organisaatiota suojautumaan potentiaalisia sovelluksista tulevia hyökkäyksiä vastaan ja tunnistamaan tietokantaan kohdistuvia hyökkäyksiä, kuten SQL-injektio ja estämään hyökkäykset, ennen kuin dataan päästään käsiksi. Lisäksi haavoittuvuudet voidaan tunnistaa sovelluskerroksella, jolloin ne voidaan korjata. (IBM Security Guardum, 2017, 5)

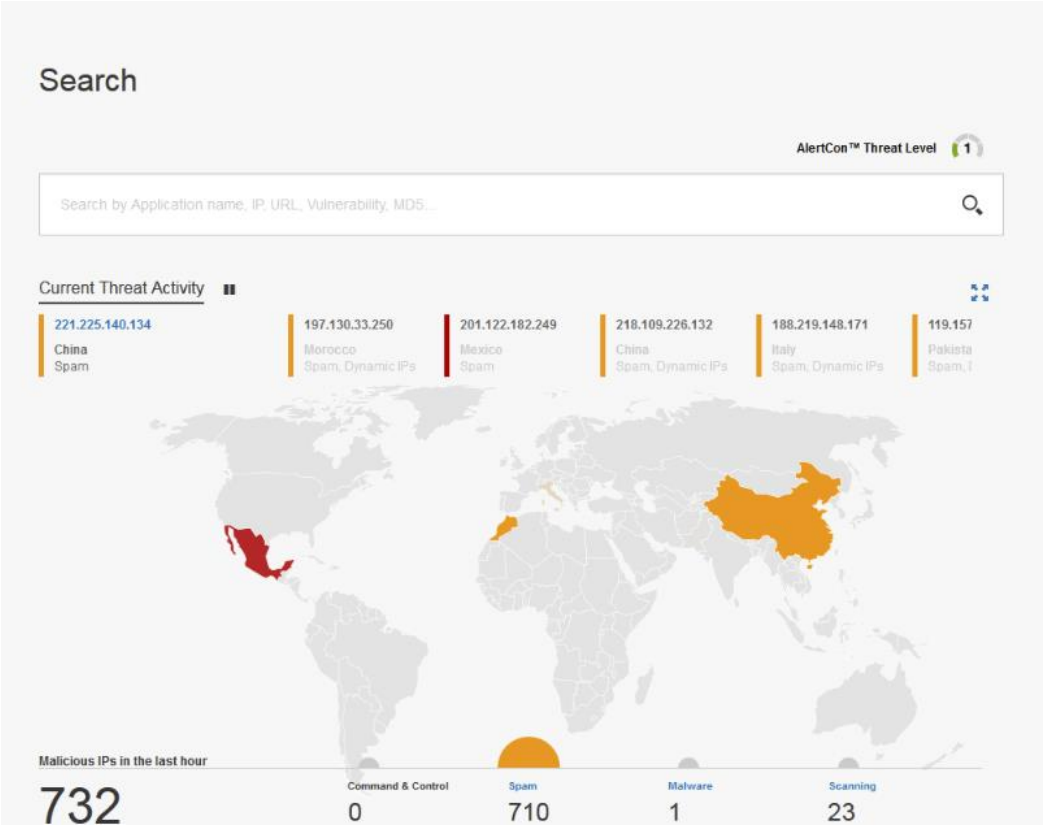
3.10.11 IBM X-Force Exchange

IBM X-Force Exchange (Kuvio 52) on pilvipohjainen kyberturvallisuusuhkia koskevan informaation jakamiseen keskittynyt alusta, joka mahdollistaa nopean globaaleihin tietoturvallisuusuhkiin keskittyvien tutkimuksien tarkastelemisen, tietoturvauhkia koskevan tietämyksen kokoamisen yhteen paikkaan, asiantuntijakonsultaatiot ja yhteistyön muiden tietoturvauhkiin keskittyvien tahojen kanssa. Alusta sisältää tällä hetkellä yli 700 teratavua raakadataa sekä reaaliaikaista tietoa tietoturvahyökkäyksistä koottuna yhteen paikkaan. Alustan avulla organisaatiot voivat tehdä yhteistyötä tietoturvauhkien vastaisessa taistelussa ja jakaa tietoa keskenään. Lisäksi Exchangen käyttäjät voivat hyödyntää IBM:n tietoturva-aineistoa sekä yhteisön jäsenten ja IBM:n asiantuntijoiden tietämystä. (IBM Viestintävirasto, 2015)

Useat yritykset hyödyntävät tietoturvauhkiin keskittyviä analyysimenetelmiä ja tietämystä tietoturvauhkista, kuten threat intelligence, jonka analyysi perustuu relevantin datan ja informaation tunnistamiseen, keräämiseen ja rikastamiseen. Yritykset usein hyödyntävät useita menetelmiä sekä tietolähteitä tietoturvauhkien tunnistamiseen, joka voi olla aikaa vievää, eikä tietolähteet ole aina luotettavia. Lisäksi yritys voi kohdata tilanteita, joissa informaatiota ei voida prosessoida riittävän nopeasti, jolloin sen hyödyntäminen käytännön tilanteissa tuottaa vain vähän hyötyä ja suojaa. (IBM X-Force Exchange Datasheet)

X-Force Exchange tarjoaa ajan tasalla olevan tietoturvauhkien analyysimenetelmiin keskittyvän alustan käyttäen pohjana ”haitakkeista”, kuten honey potista, darknetista ja spam trapista, saatua dataa. Alusta on yksi laajimmista ja kattavimmista haavoittuvuuspankeista ja se kykenee analysoimaan päivittäin tuhansia haitallisia indikaattoreita tunnissa, alustalla olevaa threat intelligence-tietämystä päivittäen. Alustassa on uhkatietopankki, joka kerää tietoa yli 15 miljardista tietoturvatapahtumasta päivittäin. Lisäksi se tarjoaa pääsyn haittaohjelmatietoihin, joita on kerätty yli 270 miljoonasta päätelaitteesta. Uhkatietoja alustaan on kerätty yli 25 miljardilta sivustolta ja se kattaa informaatiota yli kahdeksasta miljoonasta haitta- ja kalasteluhyökkäyksestä sekä yli miljoonasta haitallisesta IP-osoitteesta, jotka ovat kategorisoituja maantieteellisen sijainnin ja vaarallisuuden mukaan. (Weisser, 2015)

Exchange-alusta on toiminnaltaan kuin moni muu sosiaalisen informaation jakamista varten toteutettu sivusto, jossa sisään kirjautuneet käyttäjät voivat etsiä, kommentoida, kerätä ja jakaa informaatiota ja muut käyttäjät voivat tarkastella ja etsiä raportteja. Alustan ”Aktiviteetti”-alueella käyttäjät voivat tarkastella viimeisimpiä haavoittuvuuksia, etsiä linkkejä tietoturva-aiheisiin blogeihin oleellisten tietoturvaan viittaavien vinkkien toivossa tai tarkastella trendikirjoituksia sekä koko yhteisön viimeaikaisia historiatietoja. Henkilökohtaisella välilehdellä käyttäjät voivat lisätä raportteja tai ladata evidenssiä ulkoisista tietolähteistä ja asettaa ne julkiseksi tai yksityiseksi. (Ziadeh, 2015)



Kuva 52 IBM X-Force Exchange käyttöliittymä (Powers, 2015)

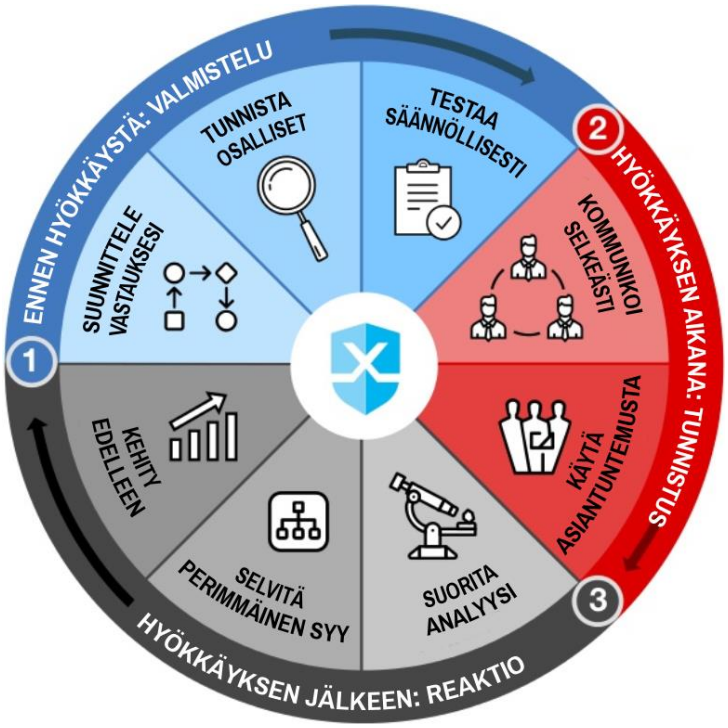
3.10.12 IBM X-Force IRIS

IBM X-Force Incident Response and Intelligence Services (IRIS) toteuttaa ennakoivaa tietoturvauhkien torjuntaa IBM X-Forcen asiantuntemusta hyödyntäen. Nykyään tietoturvauhkat tai muut haitalliset hyökkäykset kohdistuvat voimakkaasti useisiin organisaatioihin, eikä yksikään organisaatio ole täysin immuuni tämänkaltaisille hyökkäyksille organisaation tietoturvaan panostamisesta huolimatta. Ongelmana on, että organisaatiot usein suuntaavat suhteettomasti resursseja tietoturvatapahtumista, kuten tietojärjestelmiä kohtaan tehdyistä hyökkäyksistä, toipumiseen ja niihin reagoimiseen jälkikäteen, vaikka organisaatioiden tulisi varautua niihin jo ennalta. IRIS tarjoaa relevanttia tilannekuvaa tietoturvatapahtumista ja strategisista korjaustoimenpiteistä, joiden avulla organisaatio voi paremmin kontrolloida tietoturvatapahtumia ja tietomurtoja. IBM:n X-Force IRIS-tietoturva-asiantuntijoista koostuva ryhmä voi tarjota kokonaisvaltaisen lähestymistavan haitallisten tietoturvatapahtumien tunnistamiseen, niihin vastaamiseen ja niiden estämiseen aiempaa tehokkaammin. (IBM_C, 2016, 1)

Haitallisiin tietoturvatapahtumiin vastaaminen on oleellista, mutta niihin valmistautuminen ennalta on huomattavasti tehokkaampaa ja se on myös kustannustehokkaampi tapa hallita tietoturvariskejä. Oikeanlaisten palveluiden ja prosessien hyödyntäminen auttaa organisaatiota tunnistamaan potentiaalisia riskejä jo ennen kuin ne tapahtuvat ja aiheuttavat tuhoa, sekä muodostamaan tilannekuva pahimmasta mahdollisesta skenaariosta ennen kuin haitalliset tietoturvatapahtumat realisoituvat. Sisällyttämällä haitallisia tietoturvatapahtumia vastaan reaktiosuunnitelman ja hyökkäyssimulaatioharjoitukset sekä aktiivisen ja jatkuvan tietoturvauhkien etsinnän, voidaan muodostaa kokonaisvaltainen tietoturvasuunnitelma, joka säästää kustannuksia ja vähentää korjaavien toimenpiteiden tarvetta. Kuviosta 53 havainnollistuu tietoturvatapahtumat ja niiden hallinta ennen hyökkäystä ja sen jälkeen. Minimaalinen valmistautuminen tietoturvauhkiin voi johtaa merkittäviin kustannuksiin ja vaatia huomattavia korjaustoimenpiteitä haitallisen tietoturvatapahtuman jälkeen. Optimaalinen skenaario muuttaa tasapainoa. Tehokas haitallisten tietoturvatapahtumien hallintaan suuntaava ohjelma ja riittävän hyvä ennakoiva valmistautuminen voivat vähentää huomattavasti korjaavien toimenpiteiden määrää esimerkiksi tietojärjestelmissä hyökkäyksen tapahduttua. (IBM_C, 2016, 2)

Kuva 53 Tietoturvatapahtumat ja niiden hallinta ennen hyökkäystä ja sen jälkeen(IBM_C, 2016, 2)

Kuviossa 54 havainnollistuu organisaation tietoturvatapahtumaa koskevat vaiheet, eli syklit, joissa ensimmäisenä vaiheena on ennen haitallista tietoturvatapahtumaa, kuten hyökkäystä oleva valmisteluaihe (engl. prepare), hyökkäyksen aikana oleva tunnistusvaihe (engl. detect) ja hyökkäyksen jälkeinen tietoturvatapahtumaa koskeva reaktiovaihe (engl. respond). Valmisteluvaiheessa suunnitellaan reaktiota hyökkäykseen ja tunnistetaan hyökkäyksen kohteena olevat sidosryhmät. IBM:n mukaan 25 %:lla yrityksistä on olemassa hyökkäyksiä koskeva reaktiosuunnitelma, jota he johdonmukaisesti toteuttavat. Tunnistusvaiheessa kommunikaation eri tahojen kanssa tulisi olla selkeää ja asiantuntemuksen tunnistusta varten olla riittävällä tasolla. IBM:n selvityksen mukaan 53 %:lla organisaatioista on ollut tietomurtoja kahden viime vuoden aikana. Reaktiovaiheessa toteutetaan haitallisen tietoturvatapahtuman aiheuttamien ongelmien analyysi, etsitään perimmäinen syy tapahtuneelle ja kehitetään puolustusta tehokkaammaksi. IBM on tutkinut, että jopa 66 %:lla organisaatioista on puutteita suunnittelussa, joka on suurin heikkous hyökkäyksiin reagoidessa.



Kuva 54 Tietoturvatapahtumien vaiheiden sykli (IBM_D, 2017)

Organisaation luodessa tehokkaan tietoturvasuunnitelman sekä seuraamalla parhaita käytänteitä ja reagoimalla haitallisiin tietoturvatapahtumiin, kuten hyökkäykset organisaatioiden tietojärjestelmiin, jo ennen niiden tapahtumista, hyökkäyksen aikana tai hyökkäyksen jälkeen, voi huomattavasti vähentää organisaation kokemia taloudellisia tappioita. Tappiot yleensä kohdistuvat henkiseen omaisuuteen, taloudelliseen liikevaihtoon, asiakasdataan tai organisaation maineeseen liiketoiminnassa. Sen sijaan ennakoivat investoinnit ajallisesti ja resurssiperäisesti haitallisia tietoturvatapahtumia kohtaan voivat auttaa organisaatiota suojaamaan toimintojaan ja markkinaosuuksiaan kohdatessa kehittyneitä tietoturvauhkia. (IBM_E, 2017)

3.10.13 IBM X-Force Red Portal

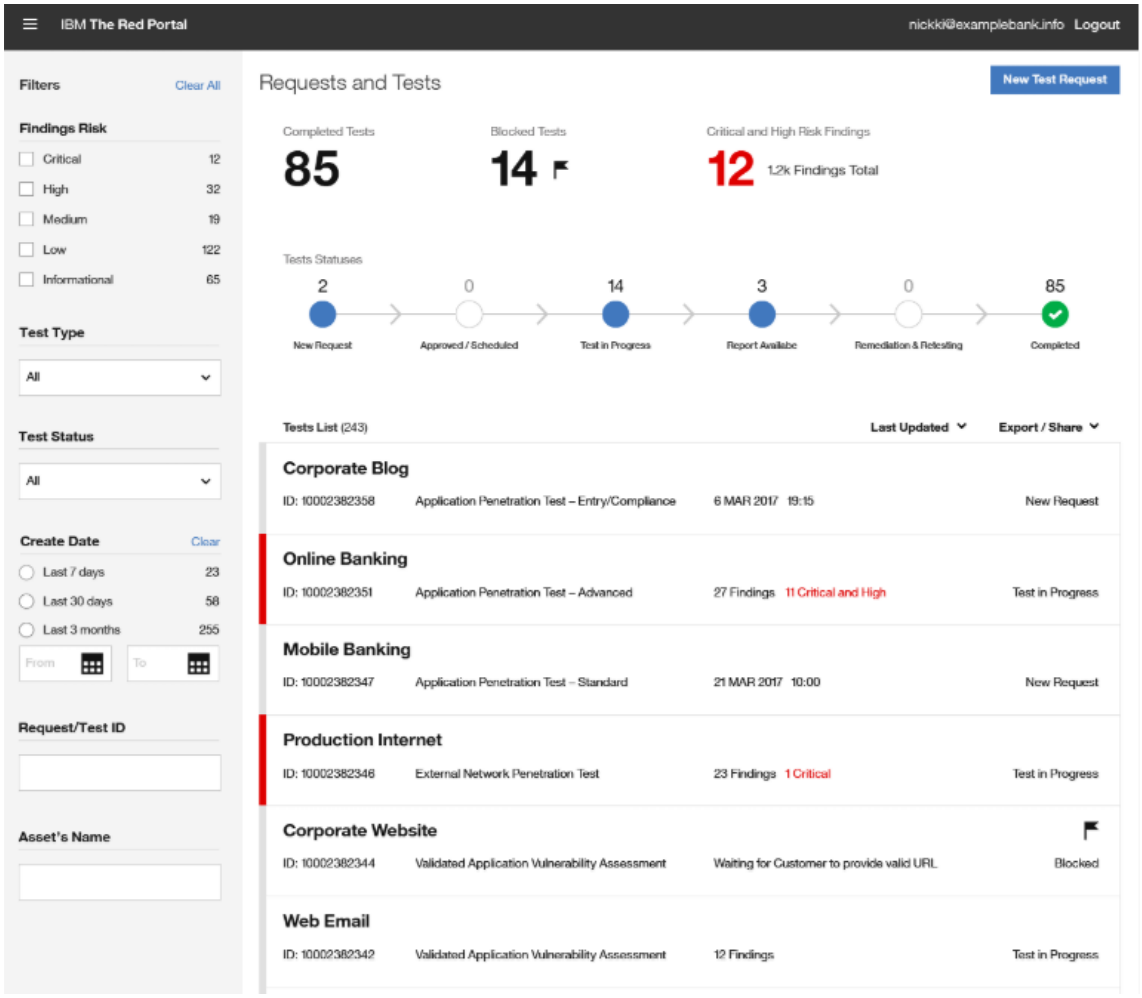
Tyytyväisyys organisaation vallitsevaan tietoturvan tason tilanteeseen käytännössä vaarantaa tietoturvan. Organisaation tietojärjestelmän arkkitehtuuriin soveltuvien tietoturvallisten laitteistojen ja ohjelmistokomponenttien asennus on tärkeää. Tärkeää on myös henkilöstön koulutus ja tietoturvasertifioinnit. Tämä ei kuitenkaan aina riitä, sillä tietoturvahyökkäyksiä suorittavat henkilöt etsivät jatkuvasti uusia aukkoja organisaatioiden tietojärjestelmäarkkitehtuurista, jotka voivat olla vanhentuneita haittaohjelmatietokantoja, laitteistojen laiteohjelmien (engl. firmware) päivityksiä, avoimeksi jääneitä portteja tai helposti arvattavia salasanoja. Toimivan tietoturvan saavuttamiseksi on tarpeen olettaa, että tietojärjestelmien läpäiseviä hyökkäyksiä tapahtuu ja niitä varten on tarpeen toteuttaa ehkäiseviä toimenpiteitä, joissa tietoturva-aukot tukitaan. (IBM Security White Paper)

IBM X-Forcen tutkijat ovat havainneet, että X-Force-portaalin asiakkaat ovat kokeneet keskimäärin 54 miljoonaa tietoturvauhkaa vuoden 2016 aikana. Ilman reaalimaailmassa tapahtuvaa testaamista, organisaatio ei käytännössä voi olla varma, kykeneekö se puolustautumaan hyökkäyksiä vastaan. Tietojärjestelmien testaaminen on jatkuva prosessi ja sen tarkoituksena on varmistaa, että jokainen tietojärjestelmän osa toimii juuri tarkoituksenmukaisella tavalla ja on ajanmukaisesti päivitetty. On oleellista tietää, kykeneekö organisaation tietoverkko estämään esimerkiksi palvelunestohyökkäyksiä tai onko organisaation tietoverkon palomuurissa, mobiiliportaalissa tai identiteetin hallinnan järjestelmässä tietoturva-aukkoja, joiden kautta hyökkääjä kykenee pääsemään sisään organisaation infrastruktuuriin. (IBM Security White Paper)

IBM X-Force Red Portal on vuonna 2017 julkaistu pilvipalvelupohjainen yhteistyö-, projektin hallinta- ja raportointiportaali, joka auttaa organisaatioita keskittymään ja hallinnoimaan tietoturvatestaukseen keskittyviä ohjelmia. Uusi portaali on tervetullut lisä X-Forcen operaatioihin, sillä ennen portaalia X-Force Red hyödynsi staattisia dokumentteja, sähköposteja, puhelinsoittoja ja joskus paikan päällä tapahtuvia tapaamisia asiakkaiden kanssa kommunikoimiseksi. Nykyäänkin X-Forcen työntekijät voivat vierailla asiakkaiden luona tai vastaanottaa puhelinsoittoja, tosin reaaliaikaisen yhteistyön toimivuus on kiistaton. Oleellista on, että asiakas otetaan mukaan tietoturvatestausprosessiin ja varmistetaan, että asiakkaalla on pääsy ja näkemys toteutetuista tietoturvatesteistä ja tietoturvatestiohjelmista. Tarvoitteena on ottaa IBM:n asiakkaat mukaan tekemään päätöksiä siitä, mitä testataan, miten ajoittaa testaaminen ja miten testien suoritus toteutetaan, sekä miten raportoida tuloksista sekä korjata ongelmat niiden ilmentyessä. (Kerner, 2017)

X-Force Red-portaali tarjoaa yksinkertaistetun ja interaktiivisen dashboard-kojelautanäkymän (Kuvio 55) organisaation tietojärjestelmien heikkouksien tarkastelua varten. Portaalin avulla organisaatiot voivat ajoittaa tietoturvatestejä aina tarpeen vaatiessa, nähdä tietoturvatestauksen tilan ja tarkastella jo saatuja tuloksia. Itse asiassa testituloksia voidaan tarkastella niin pian kuin testien suorittaja on ne dokumentoinut ja jopa ennen kuin koko tietoturvatestaus on valmistunut. Tämä mahdollistaa korjaustoimenpiteiden aloittamisen mahdollisimman aikaisessa vaiheessa ja ehkäisee useiden viikkojen

odottelun ja reagoinnin testituloksien löydöksiin. Lisäksi Red Portal kerää ja tallentaa informaatiota, jolloin historiatietojen perusteella organisaatio kykenee tarkastelemaan tietoturvatestauksen prosessin edistymistä. (IBM X-Force Red)



Kuva 55 IBM X-Force Red Portal dashboard-kojelautanäkymä (Safi, 2017)

YHTEENVETO

Tämän raportin tarkoituksena oli tarkastella, miten tekoälyä voidaan hyödyntää kyberturvallisuuden alueella esimerkiksi ennustamaan ja estämään tietoverkkoihin kohdistuvia hyökkäyksiä, tunnistamaan ja priorisoimaan mahdollisia tietoturvauhkia sekä löytämään potentiaalisia anomalioita. Koneoppimiseen perustuva anomalioiden tunnistus voi jossain tapauksissa antaa vääriä positiivisia tuloksia, jotka voivat aiheuttaa epäluottamusta järjestelmää kohtaan. Manuaalinen tulosten läpikäynti lisää ihmistyövoiman tarvetta. Parhaimmillaan tekoäly voi toimia ongelmanratkaisijan asemassa, eikä se pelkästään sisällä uhka- ja riskitekijöitä. Usein kuitenkin yhä vielä tarvitaan sekä ihmisen että koneen yhteistoimintaa tietoturvaan kohdistuvien ongelmien ratkaisemiseksi, tosin kone voi toimia merkittävänä apuna tässä kontekstissa.

Nykyään suurin haaste kyberturvallisuuden uhkien hallinnassa on tehokkaasti toimivan kyberhyökkäyksien tunnistamisiin keskittyvän kyvykkyyden puute. Avaintekijänä tunnistusprosessissa on ihmiselementin vähentäminen, jolloin inhimilliset virheet vähenevät. Tunnistusprosessi voi keskittyä tunnistusteknologioiden (allekirjoitukset, mallit jne.) tai tietoturvatapahtumiin vastaavien tekniikoiden (incident response techniques), kuten ihmisasiantuntijuuden hyödyntämiseen uhkien tunnistamiseksi tai hyökkäyksien torjumiseksi tietoverkon tai tietojärjestelmien tasolla. Tässä kontekstissa voidaan hyödyntää automaatiota ja kognitiivisia menetelmiä. Koneoppimisen ja tekoälyn tarjoamista hyödyistä kyberuhkien hallinnassa on julkaistu useita tieteellisiä artikkeleita ja konferenssiesityksiä, jotka tarjoavat aihealueen käsittelylle tieteellistä pohjaa.

Tämän raportin alussa määriteltiin, mitä tekoäly tarkoittaa, tekoälyn tarjoamia hyötyjä ja haittoja, erilaisia menetelmiä aina neuroverkoista syväoppimiseen ja niiden hyödyntämisen alueita. Tärkeänä aihealueena raportissa on koneoppiminen (ohjaamaton ja ohjattu), jota on hyödynnetty raportissa tarkastelluissa ratkaisuissa. Raportissa kuvattiin lisäksi, miten kyberturvallisuus on kehittynyt ajan saatossa suurtietokoneiden aikakauden tietoturvaratkaisuista nykyajan Internet-aikakaudelle, jossa hyödynnetään kehittyneitä sekä osin myös tekoälyä hyödyntäviä tietoturva- ja kyberturvallisuusratkaisuja. Tähän kategoriaan liittyviä ratkaisuita käsiteltiin raportin viimeisessä luvussa. Luvussa käsiteltiin yhdeksää tietoturva- ja kyberturvallisuusratkaisua, joista IBM:n ratkaisu on kokonaisvaltaisin kattaen tietoverkon turvaamisen aina mobiililaitteista, sovelluksista loppukäyttäjiin saakka.

Raportissa tarkasteltiin yhdeksää eri valmistajan toteuttamaa tekoälyä hyödyntävää kyberturvallisuusratkaisua, jotka olivat PatternEx AI2, Amazon Macie, Cyberlytic, CylanceProtect, Darktrace, Deep Instinct, SparkCognition DeepArmor, Vectra Networks Cognito ja kokonaisvaltainen IBM Security-tietoturvaratkaisu. Useimmat tarkastelluista ratkaisuista hyödyntävät koneoppimista sekä analytiikkaa kyberhyökkäysten ja -hälytysten tunnistamiseksi, niiden torjumiseksi ja niistä toipumiseksi. Darktrace-ratkaisu on muista sikäli poikkeuksellinen, että sen avulla voidaan havaita ja tunnistaa kehittyviä kyberuhkia, joihin perinteiset tietoturvallisuusratkaisut eivät ole tehonneet. Darktrace käyttää

koneoppimista ja matemaattisia malleja hyödyntävää Enterprise Immune System –teknologiaa, jonka avulla voidaan seurata käyttäytymistä ja poikkeavuuksia tietoverkoissa. EIS kykenee automaattisesti ja mukautuen oppimaan jokaisen käyttäjän, laitteen ja verkon tavan toimia. Tällöin se kykenee tunnistamaan käyttäytymismalleja, jotka ilmentävät todellisia kyberuhkia. Darktracen käyttöliittymä on graafinen sekä interaktivinen mahdollistaen uhkien visualisoinnin. Darktracen avulla yrityksillä on kattava näkyvyys verkon toimintaan ja ne voivat vastata ennakoivasti uhkiin ja pienentää riskejä. Kattavan näkökulman uhkien kartoittamiseen tuo DeepArmor-sovellus, joka kartoittaa luonnollisen kielen prosessointia hyödyntäen uhkien ympäristössä olevaa kontekstia lukien tuhaksia sivuja relevanttia informaatiota uhkista. Informaatiosta koostetaan riskiarvio ja tuotetaan uhka-analyysiyhteenveto, jonka avulla muodostetaan toimintastrategia ja puututaa relevantteihin ongelmiin.

Käyttäjät voivat käyttäytymisellään aiheuttaa potentiaalista riskiä organisaation tietoturvalle, jolloin käyttäytymisen analysointiin kehitetyt tekoälyä hyödyntävät ratkaisut ovat oleellisia. Amazon Macie toteuttaa koneoppimista hyödyntävän sensitiivisen datan luokittelun lisäksi käyttäjien käyttäytymisen analysointia tunnistamaan epäilyttävää aktiviteettia kyeten monitoroimaan, miten tekijänoikeussuojattua materiaalia kopioidaan, siirretään tai tarkastellaan. Cyberlytic Profiler toteuttaa käyttäytymisen analysointia Web-liikenteestä hyödyntäen Web-sovellusta ja ohjaamatonta koneoppimista analysoimaan datavirtoja. Vectra Networks Cognito tunnistaa hyökkääjän verkkokäyttäytymisen kyberhyökkäysketjun eri vaiheissa verraten sitä normaaliin palvelimien kanssa tapahtuvaan verkkokäyttäytymiseen. Tunnistamisen painopisteenä ovat ne, jotka ovat osa koordinoitua hyökkäyskampanjaa.

Tekoälyä voidaan hyödyntää myös haittaohjelmien tunnistamisessa kerätentä esimerkiksi nimiä ja salasanoja, jotka lähetetään edelleen hämäräperäisille sivustoille. Tällaisten sivustojen kautta kerättyä informaatiota voidaan hyödyntää tulevissa kyberhyökkäyksissä. Tässä raportissa esiteltiin CylanceProtect-työkalua, joka hyödyntää tekoälyä tunnettujen ja tuntemattomien haittaohjelmien suorituksen estämiseen päätelaitteissa. Tekoäly auttaa tarkastamaan kaikki sovellukset, joita päätelaitteissa ajetaan ja tunnistaa muistin hyväksikäytön auttaen haittaohjelmien identifioinnissa. Sovellus hyödyntää syväoppimisen algoritmeja, joiden avulla voidaan tunnistaa haittaohjelmiin viittaavia rakenteita, jolloin jo haittaohjelmien alkuvaiheen toimintaan voidaan puuttua. Sovelluksen toteutuksessa rakennettiin laboratorio-olosuhteissa neuroverkko, jonka opetuksessa käytettiin suuria määriä haitallisia ja harmittomia tiedostoja, jolloin saatiin aikaiseksi ennustemalli, joka voidaan lähettää suojattavalle laitteelle haittaohjelmien reaaliaikaista tunnistamista ja estämistä varten.

Raportissa tarkasteltu PatternEx:n A2-alustaan perustuva ratkaisu on sikäli edistyksellinen, että se mahdollistaa tietoturvahyökkäyksien ennustamisen muita tarkasteltuja ratkaisuita paremmin. Ratkaisu hyödyntää ohjaamatonta koneoppimista, jonka jälkeen tulokset esitetään analyytikoille ohjatun oppimisen mallin rakentamiseksi. Ratkaisussa analyyttisen mallin muodostamiseksi hyödynnetään sekä historiallisesta datasta koostuvaa opetusjoukkoa, että datajoukon luonnollisten kuvioiden tutkimusta ja erilaisia yhteyksiä. Pelkästään ohjaamatonta koneoppimista hyödyntämällä voitiin tutkimuksien

mukaan yltää vain 73,5 % hyökkäyksien tunnistamisasteeseen, väärien hälytysten ollessa yli 22 % epäilyttävistä tapahtumista. Ohjatun oppimisen mallin tuoma lisä nosti tunnistamistarkkuuden aina 85 % luokkaan asti. Edellä mainittu koneoppimisen menetelmien yhdistäminen analyyttisen mallin muodostamiseksi voisi tuoda lisäarvoa myös muissa tietoturvallisuuteen liittyvien ratkaisujen toteutuksissa.

Muista tässä raportissa tarkastelluista ratkaisuista poiketen IBM Security-tietoturvaratkaisu on kokonaisvaltainen ja se tarjoaa yhden maailman kehittyneemmistä ja integroiduista portfolioratkaisuista organisaatioiden tietoturvatuotteissa ja palveluissa. Portfolioratkaisu, jota tukee IBM X-Force tutkimus- ja kehitysyksiköt, tarjoaa kyvykkyyksiä, jotka kokonaisvaltaisesti tukevat ihmisten, infrastuktuurin, datan ja sovelluksien tietoturvaa. IBM Security tarjoaa kyvykkyyksiä identiteetin ja käytön hallintaan, tietokannan tietoturvallisuuteen, sovelluskehitykseen, riskien hallintaan, loppukäyttäjien hallintaan, tietoverkon tietoturvaan jne. Security-ratkaisun tarjoamat kyvykkyydet hallitsemaan riskejä ja muodostamaan integroidun tietoturvaratkaisun mobiililaitteille, pilvipalveluille, sosiaaliselle medialle ja yritysten liiketoiminta-arkkitehtuureille. IBM Security-tieturvaratkaisun etuna on keskitetty käyttöliittymä tietoturvaprofiileiden ja käytänteiden hallintaan heterogeenisistä keskuskonejärjestelmistä, hajautettuihin ja loppukäyttäjien käyttämiin IT-järjestelmiin asti. Security-ratkaisun keskiössä on IBM Watson-tekoäly.

Lähteet

Kirjallisuus, artikkelit

Bayuk, J., L., Healey, J., Rohmeyer, P., Sachs, M., H., Schmidt, J. & Weiss, J. 2012. Cyber Security Policy Guidebook. USA: A John Wiley & Sons, Inc.

Bell, J. 2014. Machine Learning: Hands-On for Developers and Technical Professionals. Wiley, 408.

Borana, J. 2016. Applications of Artificial Intelligence & Associated Technologies. Department of Electrical Engineering, Jodhpur National University. Proceeding of International Conference on Emerging Technologies in Engineering, Biomedical, Management and Science.

Brenner, W. 2010. Cybercrime – Criminal Threats from Cyberspace. Santa Barbara, California, USA: ABC-CLIO LLC.

Dale. R. 1995. An Introduction to Natural Language Generation. ESSLI.

Goodfellow, Bengio & Courville. 2016. Deep Learning. USA: MIT Press, 755.

Kiravuo,T., Särelä, M. ja Manner J. 2013. Kybersodan taistelukentät, Sotilasaikakauslehti 3/2013

Kääriäinen J. 2010. Verkkorikollisuuden vaarat, Haaste 3/2010

Lehto, M. 2014. Kybertaistelun toimintaympäristön teoreettinen tarkastelu kirjassa Kybertaistelu 2020 (Tuija Kuusisto Edit.) Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, n:o 1. 67-89

Lehto, M. 2017. Tekoäly ja turvallisuus, Futura 2/2017. 6 - 14

Lehto, M. & Limnéll, J. 2017. Kybersodankäynnin kehityksestä ja tulevaisuudesta, kirjassa M. Silvasti (Edit.) Tiede- ja Ase 2017, 179 - 212

Lehto, M. & Neittaanmäki, P. 2015. Cyber Security: Analytics, Technology and Automation. Intelligent Systems, Control and Automation: Science and Engineering. Berlin, Heidelberg: Springer International Publishing.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Saarijärvi: Docendo

Ottis R. 2008. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Proceedings of the 7th European Conference on Information Warfare and Security University of Plymouth, UK, 30 June – 1 July 2008. 163 - 167

Veeramachaneni, K., Arnaldo, I., Cuesta-Infante, A., Korrapati, V., Bassias, C. & Li, K. 2016. Ai2: Training a Big Data Machine to Defend. Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing (HPSC), IEEE International Conference on Intelligent Data and Security (IDS), IEEE 2nd International Conference on Intelligent Data and Security (IDS). New York: USA.

Zhao, R., Song, W., Zhang, W., Xing, T., Lin, J., Srivastava, M., Gupta, R. & Zhang, Z. 2017. Accelerating Binarized Convolutional Neural Networks with Software-Programmable FPGAs. Proceedings of the 2017 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays, 15 - 24, Monterey, California, USA.

Internet-lähteet

Akagi, D. 2014. A Primer on Deep Learning. Viitattu 16.5.2017 https://www.dataro-bot.com/blog/a-primer-on-deep-learning

Arboleda, N. 2017. Deep Learning Cybersecurity Provider Deep Instinct Launches Australian Operations. Viitattu 2.2.2017 https://www.crn.com.au/news/deep-learning-cybersecurity-provider-deep-instinct-launches-australian-operations-478594

Amazon Macie FAQ. 2018. What is Amazon Macie? Viitattu 14.3.2018 https://aws.amazon.com/macie/faq

Audet, S. 2014. New Intelligence Analytics Uncover Hidden Criminal Activity in Just Seconds. Physorg. Viitattu 16.5.2018 http://phys.org/pdf333702867.pdf

Bask, J. & Nuopponen, A. 1998. Neuroverkot. Teknillinen korkeakoulu. Viitattu 17.5.2017 http://www.tml.tkk.fi/Studies/Tik-110.300/1998/Newtech/neuro-verkot_3.html

Bell, K. 2017. Rythm Unveils AI Platform Morpheo to Help Diagnose Sleep Disorders. Viitattu 3.5.2017 http://www.firstwordmedtech.com/node/995566?re-gion_id=3

Brownlee, J. 2016. What is Deep Learning? Viitattu 16.5.2017 http://machinelearning-mastery.com/what-is-deep-learning

Bruce, 2016. IBM Resilient – Introducing: The Industry's First Security Incident Visualization. Viitattu 18.6.2018 https://www.resilientsystems.com/cyber-re-silience-knowledge-center/incident-response-blog/introducing-industrys-first-security-incident-visualization

Buczkowski, A. 2017. What's the Difference Between Artificial Intelligence, Machine Learning and Deep Learning? Viitattu 31.5.2017 http://geoawesome-ness.com/whats-difference-artificial-intelligence-machine-learning-deep-lear-ning

Butcher, S. 2017. J.P.Morgan's Massive Guide to Machine Learning and Big Data Jobs in Finance. Efinancial Careers. Viitattu 27.12.2017 https://news.efinancialca-reers.com/uk-en/285249/machine-learning-and-big-data-j-p-morgan

Choilawala, M. & Ramesh, R. 2015. IBM BigFix – Bridging the Endpoint Gap Between IT Ops and Security. IBM Security. Viitattu 22.5.2018 https://www.slideshare.net/ibmsecurity/bridging-gap-between-security-defenses-and-critical-data

Condliffe, J. 2016. Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks. MIT Technology Review. Viitattu 25.6.2018 https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks

Conner-Simons, A. 2016. System Predicts 85 Percent of Cyber-Attacks Using Input from Human Experts. Viitattu 7.3.2018 https://phys.org/news/2016-04-percent-cyber-attacks-human-experts.html

Copeland, M. 2016. What's the Difference Between Artificial Intelligence, Machine Learning, and Deep Learning. Viitattu 16.5.2017 https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai

Cyberlytic. The Profiler – AI for Web Security Technical Data Sheet. Viitattu 9.1.2018 https://www.cyberlytic.com/uploads/resources/Technical-Data-Sheet-Final.pdf

Cyber Threat Hunting. 2017. IBM i2 Enterprise Insight Analysis or Cyber Intelligence – IBM i2 Enterprise Insight Analysis Can Help You Fortify Your Cybersecurity by Uncovering Hidden Threats, Buried in Data, in Near Realime. IBM Corporation. Viitattu 16.5.2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZZS03196USEN

Darktrace. 2018. Threat Detection and Classification. Viitattu 31.1.2017 https://www.darktrace.com

DeepArmor. 2018. A Cognitive Approach to System Protection – Raise Malware Prevention to a Cognitive Level. Viitattu 12.3.2018 https://www.sparkcognition.com/deep-armor-cognitive-anti-malware

Deretsky, Z. NFS and the Birth of the Internet. National Science Foundation. Viitattu 4.12.2018 https://www.nsf.gov/news/special_reports/nsfnet/60s_to_90s_map.pdf

Dettmers, T. 2015. Deep Learning in a Nutshell: Core Concepts. Viitattu 17.5.2017 https://devblogs.nvidia.com/parallelforall/deep-learning-nutshell-core-concepts

Dheap, V. 2017. IBM QRadar Advisor with Watson: Revolutionizing the Way Security Analysts Work. Security Intelligence. Viitattu 4.12.2018 https://securityintelligence.com/ibm-qradar-advisor-with-watson-revolutionizing-the-way-security-analysts-work

G2 Growd. 2018. Best Security Information and Event Management (SIEM) Software. Viitattu 4.8.2018 https://www.g2crowd.com/categories/security-information-and-event-management-siem

GeeksforGeeks. Artificial Intelligence | Natural Language Generation. A Computer Science Portal for Geeks. Viitattu 30.3.2018 https://www.geeksforgeeks.org/artificial-intelligence-natural-language-generation

Holm. P. 2018. Watson Kista Summit 2018 – Innovera för en Ny Säkerhetsverksamhet. Viitattu 4.9.2018 https://www.slideshare.net/ibmsverige/kista-watson-summit-final-public-version

IBM Advanced Incident Response Orchestration. Accelerate Response with the Industry's Most Advanced Orchestration Platform. Viitattu 18.6.2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=47016547USEN&

IBM. Watson for Cyber Security in Action. Viitattu 15.5.2018 https://as-cc.com/ibmshowcase/index.php?zCustomPage=IBM%20Security%20QRadar%20Advisor%20with%20Watson

IBM_B. Preparing for GDPR Compliance with Endpoint and Mobile. Viitattu 20.5.2018 https://reviews.financesonline.com/p/ibm-maas360

IBM_C. 2016. Proactively Tackle Security Threats with IBM X-Force Skills and Expertise. IBM X-Force Incident Response and Intelligence Services Helps Organizations Prepare for, Prevent, Detect and Respond to Security Incidents. IBM Solution Brief. Viitattu 19.6.2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SES03030USEN&

IBM_D. 2017. Before, During and After an Attack. Security Intelligence. Viitattu 19.6.2018 https://securityintelligence.com/media/dealing-with-attacks-and-applying-an-effective-incident-response-methodology

IBM_E. 2017. Dealing with a Data Breach: Before. During. After – Best Practices for Improving Your Incident Response Processes. IBM Security. Viitattu 19.6.2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEW03151USEN&

IBM MaaS360. 2018. IBM MaaS360 Review. Financesonline. Viitattu 20.5.2018 https://reviews.financesonline.com/p/ibm-maas360

IBM QRadar Advisor with Watson. What Can Artificial Intelligence Do for Security Analysts? Viitattu 15.5.2018 https://www.ibm.com/us-en/marketplace/cognitive-security-analytics

IBM QRadar Incident Forensics. Quickly Conduct Network Forensics Investigations. Viitattu 31.5.2018 https://www.ibm.com/us-en/marketplace/ibm-qradar-incident-forensics

IBM QRadar Network Insights. What It Can Do for Your Business. Viitattu 31.5.2018 https://www.ibm.com/us-en/marketplace/real-time-threat-identification

IBM QRadar SIEM. 2014. Detect Threats with IBM QRadar Security Information and Event Management (SIEM). IBM Security Data Sheet. Viitattu 7.8.2018 http://www.sia.es/Documents/assets/datasheet-qradar-wgd03097usen.pdf

IBM Resilient. 2018. IBM Resilient – incident Response. Infoguard, Swiss Cyber Security. Viitattu 18.6.2018 https://www.infoguard.ch/en/partners/ibm-resilient-incident-response

IBM Resilient Incident Response Platform. 2017. Resilient Incident Platform Overview. Accelerate Your Response with an Advanced, Battle-tested Platform for Incident Response Orchestration. Viitattu 18.6.2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=46016546USEN&

IBM Security AppScan Enterprise. 2012. Application Security Testing and Risk Management. IBM Software Application Security. Viitattu 11.6.2018 http://ibm.con-res.com/wp-content/uploads/2017/06/ibm-appscan-enterprise-datasheet.pdf

IBM Security. 2016. Let's Talk About Apps & Extensions for QRadar. IBM Security Support Open Mic. Viitattu 26.6.2018 http://www-01.ibm.com/support/docview.wss?uid=swg27048509&aid=1

IBM Security. 2018. QRadar Advisor with Watson. Viitattu 15.5.2018 https://exchange.xforce.ibmcloud.com/hub/extension/2cd0b0f8d77a9c73b278fbc424e8eb6a

IBM Security Guardum. 2017. Secure the Data That Power Your Business. IBM Security Guardum Helps Analyze, Protect and Adapt for Comprehensive Data Protection. IBM Security Solution Brief. Viitattu 4.6.2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&htmlfid=WGS03063USEN&attachment=WGS03063USEN.PDF

IBM Security White Paper. Preempt Attacks with Programmatic and Active Testing – Prove Your Network, Systems and Data Security with IBM X-Force Red Penetration Testing. IBM Security White Paper. Viitattu 10.6.2018 https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03161usen/security-ibm-security-services-se-white-paper-external-sew03161usen-20170728.pdf

IBM Security zSecure Admin. What zSecure Admin Can Do for Your Business. Viitattu 3.8.2018 https://www.ibm.com/fi-en/marketplace/zsecure-admin

IBM Security zSecure Alert. What zSecure Alert Can Do for Your Business. Viitattu 9.7.2018 https://www.ibm.com/fi-en/marketplace/zsecure-alert

IBM Security zSecure Audit. What zSecure Audit Can Do for Your Business. Viitattu 9.7.2018 https://www.ibm.com/fi-en/marketplace/zsecure-audit

IBM Security zSecure CICS Toolkit. What zSecure CICS Toolkit Can Do for Your Business. Viitattu 3.8.2018 https://www.ibm.com/us-en/marketplace/zsecure-cics-toolkit

IBM zSecure Command Verifier. zSecure Command Verifier Enforces Security Policies. Viitattu 9.7.2018 https://www.ibm.com/fi-en/marketplace/command-verifier

IBM Security zSecure Suite. 2017. An Interactive Guide to IBM Solutions for Managing and Maintaining Security on the Mainframe. IBM Security. Viitattu 3.7.2018 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03210USEN&attachment=WGW03210USEN.PDF

IBM Viestintävirasto. 2015. IBM Avaa Pilvipohjaisen Yhteistyöalustan Ja Tuo Uhkien Analytiikan Pilveen Kyberrikollisuuden Nujertamiseksi. Viitattu 15.5.2018 https://www.mynewsdesk.com/fi/ibmfinland/news/ibm-avaa-pilvipohjaisen-yhteistyoealustan-ja-tuo-uhkien-analytiikan-pilveen-kyberrikollisuuden-nujertamiseksi-119850

IBM User Guide. 2018. IBM QRadar User Behavior Analytics (UBA) app Version 2 Release 7. Viitattu 25.6.2018 https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.UBAapp.doc/b_Qapps_UBA.pdf?view=kc

IBM X-Force Exchange Datasheet. 2017. IBM X-Force Exchange Is a Cloud-Based Threat Intelligence Sharing Platform. Viitattu 15.5.2018 https://www01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=SP&htmlfid=WGD03055USEN

IBM X-Force Red. X-Force Red Penetration Testing – Test Your Applications, Network, Hardware and More to Defend Against Attacks. IBM Security. Viitattu 10.6.2018 https://www.ibm.com/security/services/penetration-testing

i-Scoop. Artificial Intelligence (AI) and Cognitive Computing: What, Why and Where. Viitattu 21.12.2017 https://www.i-scoop.eu/artificial-intelligence-cognitive-computing

ITU. 2018. Definition of Cyber Security. Viitattu 8.1.2018 https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Jain, K. 2015. Machine Learning Basics for a Newbie. Analytics Vidhya. Viitattu 27.12.2017 https://www.analyticsvidhya.com/blog/2015/06/machine-learning-basics

Kannan, P., V. 2017. Artificial Intelligence – Applications in Healthcare. Asian Hospital & Healthcare Management. Viitattu 30.5.2017 https://www.asianhhm.com/technology-equipment/artificial-intelligence

Kasperskylab. 2018. What is Cyber-Security? Viitattu 8.1.2018 https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kerner, S., M. 2017. IBM X-Force Red Provides Collaboration Portal for Security Testing. Viitattu 10.6.2018 http://www.eweek.com/security/ibm-x-force-red-provides-collaboration-portal-for-security-testing

Kinnunen, Y. 2017. SIEM-järjestlemä on Organisaation Kyberturvallisuuden Hermokeskus. Insta Group. Viitattu 18.6.2018 https://www.insta.fi/medialle/tiedotteet-ja-artikkelit/insta-defsec/2017/08/siem-jarjestelma-on-organisaation-kyberturvallisuuden-hermokeskus.html

Kyberturvallisuus. 2018. Haavoittuvuudet. Viitattu 14.3.2018 https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet.html

Lehto, M. 2016. Kyberturvallisuuden tuottaminen. Luento, Jyväskylän yliopisto. Viitattu 4.12.2018 https://peda.net/jyu/it/do/kkv/ajankohtaista/mlkt

Lord, N. 2017. What is Cyber Security? Data Insider. Viitattu 8.1.2018 https://digitalguardian.com/blog/what-cyber-security

Lumen. Evidence-Based Decision Making. Principles of Management. Viitattu 9.5.2018 https://courses.lumenlearning.com/wm-principlesofmanagement/chapter/evidence-based-decision-making

Managed Security Services. Strengthen Your Information Security Defences and Lower Costs. IBM Security. Viitattu 31.5.2018 https://www-03.ibm.com/security/uk-en/services/managed-security-services

MI5. 2018. Security Service – Cyber. Viitattu 11.1.2018 https://www.mi5.gov.uk/cyber

Murphy, D. 2017. BigFix and QRadar Integration – Incorporating BigFix Endpoint Intelligence in QRadar. IBM Community. Viitattu 22.5.2018 https://ibm.co/2mkpCrA

Naik, D. 2017. Understanding Recommendation Engines in AI. Humans for AI. Viitattu 23.4.2018 https://medium.com/@humansforai/recommendation-engines-e431b6b6b446

Northdoor, 2018. Harmonise Your Security Process with Orchestrated Incident Response. IBM Resilient Response Platform. Viitattu 18.6.2018 https://www.northdoor.co.uk/ibm-resilient-incident-response

Palmer, T. 2017. Vectra Cognito – Automating Security Operations with AI. ESG Lab Review. Viitattu 7.2.2018 https://info.vectra.ai/hs-fs/hub/388196/file-1918923738.pdf

Patel, M. 2017. QRadar UBA App Adds Machine Learning and Peer Group Analyses to Detect Anomalies in User's Activities. Viitattu 25.6.2018 https://securityintelligence.com/qradar-uba-app-adds-machine-learning-and-peer-group-analyses-to-detect-anomalies-in-users-activities

Parloff, R. 2016. Why Deep Learning is suddenly Changing Your Life. Viitattu 16.5.2017 http://fortune.com/ai-artificial-intelligence-deep-machine-learning

Patel, S. & Pingel, J. 2017. Introduction to Deep Learning. What are Convolutional Neural Networks? Viitattu 19.12.2017 https://se.mathworks.com/videos/introduction-to-deep-learning-what-are-convolutional-neural-networks--1489512765771.html

Powers, C. 2015. Introducing IBM X-Force Exhcange. Viitattu 15.5.2018 https://www.ibm.com/developerworks/community/blogs/81c130c7-4408-4e01-adf5-658ae0ef5f0c/entry/introducing_ibm_x_force_exchange?lang=en

Sarkar, S. 2016. How to Use Machine Learning in Today's Enterprise Environment. Viitattu 16.5.2017 http://readwrite.com/2016/11/09/machine-learning-used-pl1

Safi, K. 2017. The Red Portal: IBM X-Force Red's Collaborative Client Experience. Security Intelligence. Viitattu 10.6.2018 https://securityintelligence.com/the-red-portal-ibm-x-force-reds-collaborative-client-experience

SAS. Machine Learning – What It Is and Why It Matters. Viitattu 16.5.2017 https://www.sas.com/en_us/insights/analytics/machine-learning.html

Secureworks. 2017. Cyber Threat Basics, Types of Threats, Intelligence & Best Practices. Viitattu 16.1.2018 https://www.secureworks.com/blog/cyber-threat-basics

Selden, H. 2016. Deep Instinct: A New Way to Prevent Malware, With Deep Learning. Viitattu 2.2.2018 http://www.tomshardware.com/news/deep-instinct-deep-learning-malware-detection,31079.html

Stergiou, C. & Siganos, D. Neural Networks. Imperial College London, Department of Computing. Viitattu 15.5.2017 https://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html#Introduction%20to%20neural%20networks

Stonefly. 2018. Amazon Macie: Artificial Intelligence for Efficient Data Security. Viitattu 14.3.2018 https://stonefly.com/blog/amazon-macie-artificial-intelligence-efficient-data-security

Thought Leadership White Paper. 2013. Creating the Ultimate Security Platform. IBM System Z Delivers Proactive Protection for Data, Web, Cloud, Mobile and Enterprise Environment. Viitattu 27.6.2018 ftp://public.dhe.ibm.com/software/os/systemz/pdf/Creating_the_ultimate_security_platform_-_White_Paper.pdf

Tiquet, A. 2017. NVIDIA Invests in Cybersecurity Startup Deep Instinct. Viitattu 2.2.2018 https://blogs.nvidia.com/blog/2017/07/12/nvidia-invests-cyber-security-startup-deep-instinct

Tjoa, S. Introduction to Deep Learning. Viitattu 16.5.2017 https://ccrma.stanford.edu/workshops/mir2013/CCRMA_MIR2013_DBN.pdf

UFLDL Tutorial. 2017. Convolutional Neural Network. Viitattu 17.5.2017 http://ufldl.stanford.edu/tutorial/supervised/ConvolutionalNeuralNetwork

Viestintävirasto. 2011. TSL-protokollaa vastaan kehitetty BEAST-hyökkäys. Viitattu 12.11.2018 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2011/09/ttn20110927116.html

Walker, M. 2013. Prescriptive Analytics. Data Science Central. Viitattu 20.3.2018 https://www.datasciencecentral.com/profiles/blogs/prescriptive-analytics

Watson for Cyber Security. 2017. IBM Watson Auttaa Tietoturva-asiantuntijoita Tunnistamaan ja Seulomaan Tietoturvauhkia. Cambridge, MA. Viitattu 31.5.2018 https://www.ibm.com/news/fi/fi/2017/02/13/ WatsonForCyberSecurity_SOC.html

Weber, D. O. 2015. 12 Ways Artificial Intelligence Will Transform Health Care. H&HN Hospitals & Health Networks. Viitattu 31.5.2017 http://www.hhnmag.com/articles/6561-ways-artificial-intelligence-will-transform-health-care

Weisser, C. 2015. X-Force Exchange Threat Intelligence Platform. Viitattu 15.5.2018 https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/x-force-exchange-threat-intelligence-platform

X-Force Exchange. 2015. IBM Avaa Pilvipohjaisen Yhteistyöalustan ja Tuo Uhkien Analytiikan Pilveen Kyberrikollisuuden Nujertamiseksi. Viitattu 31.5.2018 https://www.ibm.com/news/fi/fi/2015/04/23/xforceexchange.html

Ziadeh, A. 2015. What 700 TB of Cyber Threat Data Can Do for You. Government Cloud Insider. Viitattu 15.5.2018 https://gcn.com/articles/2015/05/08/x-force-threat-intell-exchange.aspx

Informaatioteknologian tiedekunnan julkaisuja
No. 60/2018

ISBN 978-951-39-7557-9 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO